2017 ANNUAL REPORT

NIST/ITL CYBERSECURITY PROGRAM

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

NIST SPECIAL PUBLICATION 800-203

THIS PAGE IS INTENTIONALLY LEFT BLANK

ANNUAL REPORT 2017

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.800-203

JULY 2018

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

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

AUTHORITY

This publication has been developed by the National Institute of Standards and Technology (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 800-203
Natl. Inst. Stand. Technol. Spec. Publ. 800-203, 175 pages (July 2018)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-203

REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

The Information Technology Laboratory (ITL) at 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 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) a Lisa Carnahan (Standards Coordination Office, NIST), for reviewing and providing valuable feedback for this annual report.

The editors would also like to acknowledge Natasha Hanacek (Graphic Designer, NIST Public Affairs Office) for designing the cover and inside layout for this 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

TABLE OF CONTENTS

WELCOME LETTER 1
ITL INVOLVEMENT WITH INTERNATIONAL IT SECURITY STANDARDS 13
RISK MANAGEMENT 19
BIOMETRIC STANDARDS AND ASSOCIATED CONFORMITY ASSESSMENT TESTING TOOLS 29
CYBERSECURITY APPLICATIONS 30
SOFTWARE ASSURANCE & QUALITY 33
FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT (R&D) 36
COMPUTER FORENSICS 36
CYBERSECURITY AWARENESS, TRAINING, EDUCATION, AND OUTREACH 38
CRYPTOGRAPHIC STANDARDS PROGRAM 45
VALIDATION PROGRAMS 61
IDENTITY AND ACCESS MANAGEMENT 74
RESEARCH IN EMERGING TECHNOLOGIES 83
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE (NCCoE) 96
INTERNET INFRASTRUCTURE PROTECTION 99
ADVANCED SECURITY TESTING AND MEASUREMENTS 102
TECHNICAL SECURITY METRICS 113
USABILITY AND SECURITY 117
ITL CYBERSECURITY PROGRAM RELATED PUBLICATIONS 129
ITL PUBLICATIONS RELEASED DURING FY 2017 141
APPENDICES 162

THIS PAGE IS INTENTIONALLY LEFT BLANK

WELCOME LETTER

If recent events involving the security of information and operations have taught us anything, it is that cybersecurity, and the way cybersecurity risks are managed, are no longer solely the domain of the information technology specialist. Cybersecurity risk management issues are becoming increasingly familiar topics in executive management offices and boardrooms. That is as true for businesses as it is for federal and other government organizations.

No doubt that is because every year brings more troubling reports of organizations experiencing financial and reputational damage from both novel and well-known threats and vulnerabilities. But what does not get nearly as much attention are the impressive advances that so many organizations have been making in thoughtfully and successfully securing their information and processes and the systems upon which those organizations, their leaders, and their customers depend.

That's where the cybersecurity work of the National Institute of Standards and Technology (NIST) comes into play. For nearly 50 years, we have been helping organizations to succeed in building the strategies and in employing the tools needed to better recognize, anticipate, and manage cybersecurity risks. Our diverse cybersecurity activities are an essential ingredient in carrying out the NIST Information Technology Laboratory's mission: *to cultivate trust in information and technology.* We do that by conducting foundational and applied cybersecurity research to produce and advance cybersecurity standards, best practices, measurements, and reference resources. While NIST has an explicit statutory mission to focus on federal government agencies, our work can and is being heavily leveraged by large and small businesses, state and local agencies, and other organizations. Ultimately, this benefits taxpayers, investors, consumers, our digital economy, and our national security.

However, we don't work alone. To the contrary, all cybersecurity efforts at NIST are based on input from, and often in cooperation with, the private sector and other government agencies.

We also don't work in the dark. NIST prides itself on being transparent, open, and collaborative. When we actively engage the private and public sectors, we rely on and use experts from around the country – and around the globe – to complement the talents of our own staff. Exposing our thinking to others helps to improve the quality, relevance, and likely use of the end product.

This report features some of our most significant accomplishments during Fiscal Year (FY) 2017 in risk management, cryptography, identity and access management, vulnerability management, education and workforce development, and internet and communications infrastructure, as well as our efforts to transition our work into common practice. Below are just a few highlights of the work carried out in 2017.

- 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. Employing NIST's proven approach of worldwide open competitions, in 2016 we solicited 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. We now are engaging the cryptographic community in the difficult work of determining how the 69 submissions we received in 2017 meet the competition's exacting requirements.
- In instances where many devices are interconnected and working in concert to accomplish some task, security and privacy can be very important but hard to achieve due to limited capabilities available to handle modern cryptographic algorithms. This includes automotive systems, sensor networks,

healthcare, distributed control systems, the smart grid, and cyber-physical systems and the Internet of Things (IoT). Recognizing this special challenge and in order to gain greater awareness and involvement with the cryptographic community, NIST shared its findings in this area (known as lightweight cryptography) and presented our plans to address standardization issues for community feedback.

- NIST improved two widely used guidelines that provide senior leaders with the information they need to make risk-based decisions affecting critical mission and business functions. We proposed revisions to *Security and Privacy Controls for Information Systems and Organizations* (Special Publication (SP) 800-53) and *Risk Management Framework for Information Systems and Organizations* (SP 800-37). The latter provides a closer link between risk management processes and activities at various organizational levels. It demonstrates how the Cybersecurity Framework can be implemented using established Risk Management Framework processes. Both publications will be finalized in 2018.

- Reflecting a growing recognition of the link between cybersecurity and privacy risk management, we collaborated with internal and external partners to integrate privacy requirements and considerations into SP 800-53 and SP 800-37 risk management guidelines as well as our latest version of NIST's *Digital Identity Guidelines* (SP 800-63-3), which covers digital identity from the initial risk assessment to the deployment of federated identity solutions. These guidelines build the foundation needed to make privacy and security equal, quality attributes in trustworthy systems. We focused on encouraging the adoption of trusted identities through digital identity standards for federal agencies and internationally.

- The supply chain that provides the information and operational technology (IT/OT) upon which we all depend has evolved into a complex, globally distributed, dynamic ecosystem enabling the development of highly refined, sophisticated, cost-effective, and reusable solutions. In FY 2017, we published a proposed process model providing a method to identify and prioritize IT/OT systems and components. The approach aims to increase an organization's ability to make cost-effective risk decisions by determining the systems and components that have the greatest impact on the organization and that would potentially cause the most harm if compromised.

- As NIST continues to collaborate with stakeholders to raise awareness and encourage the use of the voluntary Cybersecurity Framework, we solicited public comments on a draft update of the first (2014) version and hosted a widely attended workshop that charted progress and shared issues to which NIST now has given additional attention. In May 2017, the President's Executive Order 13800 directed federal agency heads to use the Cybersecurity Framework to manage cybersecurity risk. In response, NIST released draft guidance on how the Risk Management Framework and Cybersecurity Framework can work together to help agencies develop, implement, and continuously improve their information security programs. After incorporating public comments, NIST released the Baldrige Cybersecurity Excellence Builder, a self-assessment tool based in part on the Cybersecurity Framework, to help organizations better understand the effectiveness of their cybersecurity risk management efforts.

- In FY 2017, NIST's National Cybersecurity Center of Excellence (NCCoE) began taking full advantage of its expanded, more capable facilities to accelerate the adoption of standards-based, security technologies. Healthcare and financial services were two areas that had notable progress, including the development of new draft practice guides on securing wireless infusion pumps and on managing access rights for the financial sector. NCCoE also leveraged industry partners' expertise to produce a guide on how organizations can develop strategies to recover operating systems, user files, applications, and other IT assets from data corruption events such as ransomware. The guide also offers insights on auditing, reporting, and investigations following a company's discovery of such destructive security incidents. Other guides addressed the authentication of mobile device users with personal identity verification credentials and how organizations can use attribute-based access controls to better manage employee access to data and networks.

- The NIST-led National Initiative for Cybersecurity Education (NICE) made noteworthy strides in FY 2017 to foster, energize, and promote a robust network and an integrated ecosystem of cybersecurity education, training, and workforce development. We published the *NICE Cybersecurity Workforce Framework*, establishing a taxonomy and common lexicon to describe all cybersecurity work and workers, irrespective of where or for whom the work is performed. NICE launched "CyberSeek,"an online tool that provides a visualization of the demand for and the supply of cybersecurity workers across the country as well as career pathways in cybersecurity. Via NICE, NIST served as the Commerce Department's lead, working with the Department of Homeland Security (DHS) to analyze U.S. cybersecurity workforce issues and offer recommendations in response to the President's May 2017 Executive Order.

Looking ahead – with full knowledge that new challenges are constantly emerging – we are moving towards collaborating with industry, government agencies, and others who use NIST's cybersecurity research, standards, and guides. For example, in FY 2018 NIST is assigning higher priority to the cybersecurity and privacy aspects of the Internet of Things (IoT). Researchers in our Cybersecurity for IoT program are working with industry to produce guidance and best practices, as well as to perform research and coordinate standards within and across sectors in the digital economy. We are reviewing international standards-based approaches to the IoT challenges and ramping up our IoT-related identity work. NIST is also launching a project to provide organizations with practical guidance to reduce the vulnerability of IoT devices to botnets and other automated distributed threats, while also limiting the utility of compromised devices to malicious actors. Such efforts are paving the way toward more secure IoT devices in the future.

In addition to the work in IoT, NIST has embarked on a project to automate much of the testing required under the cryptographic validation programs. We expect that automated cryptographic algorithm testing will be complete in 2018, and we will then begin developing methods to automate the testing of cryptographic modules. These efforts in automation are intended to provide a higher trust in the assurance claims made by the product developers, but do so in an efficient, and cost-effective manner that allows the vendors' conformance efforts to keep pace with the changing IT landscape. By investing in a more robust testing infrastructure, NIST hopes that product vendors will take advantage of this service by validating their products more often, which will produce more secure products.

In reporting on our accomplishments, NIST welcomes all suggestions about how we can improve our work. We do this so that we can provide the nation with the kind of cybersecurity information and tools needed to cultivate trust in information and technology while advancing and protecting our economy and our nation.

All projects in this report include contact information for the key NIST contacts. Let us hear from you.

Donna F. Dodson,
NIST Chief Cybersecurity Advisor

BACKGROUND INFORMATION OF ANNUAL REPORT

This Annual Report provides the opportunity to describe the many cybersecurity program highlights and accomplishments from throughout the NIST Information Technology Laboratory (ITL). The report is organized into several sections, each section is identified by a title page.

Please note: This Annual Report covers the Federal Government's Fiscal Year (FY) 2017, from October 1, 2016 to September 30, 2017.

ITL, an operating unit under NIST, contains seven divisions. Cybersecurity work is conducted by each, and is the sole focus of the Applied Cybersecurity and Computer Security Divisions. Throughout this Annual Report, there are references to particular division activities, and often to work by groups within those divisions. Primarily, the authors of each segment of the report have attributed accomplishments to ITL, since the 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 requests 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) OFFICE

Charles Romine, *Director*
Jim St. Pierre, *Deputy Director*

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

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

Applied and Computational Mathematics Division (ACMD)
Ronald F Boisvert, *Division Chief*

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

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

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

ITL's Cybersecurity Program is pleased to share these achievements and accomplishments made during the 2017 Fiscal Year in this Annual Report.

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 2017 by the ITL Cybersecurity Program. Detailed explanations of these activities are provided in the next section.

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 (ITL). There are multiple divisions within ITL that are involved with cybersecurity programs and 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 FY 2017, the ITL Cybersecurity Program addressed its assignment through the following major activities:

- **Forty-one NIST Special Publications (SP) (20 approved as final and 21 drafts) were issued, providing management, operational, and technical security guidelines in a variety of topic areas, including:**
  The 2016 Annual Report, the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, attribute-based access control and access control standards and policies, application container security, Secure Hash Algorithm-3 (SHA-3) derived functions, cybersecurity event recovery, data integrity, recovering from ransomware and other destructive events, securing Apple OS X 10.10 systems, protecting controlled unclassified information in nonfederal information systems and organizations, systems security engineering, cyber threat information sharing, bluetooth security, the National Checklist Program, digital identity guidelines, block cipher modes of operation, the Cipher-Based Message Authentication Code (CMAC) - a Mode for Authentication, an introduction to information security, a report of the workshop on software measures and metrics to reduce security vulnerabilities, platform firmware resiliency, fog computing, de-identifying government datasets, Long Term Evolution (LTE) security, trustworthy email, security recommendations for hypervisor deployment, the Triple Data Encryption Algorithm (TDEA) Block Cipher, key-derivation methods in key-establishment schemes, pair-wise key-establishment schemes using discrete logarithm cryptography, security and privacy controls, a risk management framework for information systems and organizations, personal identity verification (PIV) credentials, access rights management for the financial services sector, securing wireless infusion pumps in healthcare delivery organizations, situational awareness for electric utilities, and domain name systems-based electronic mail security.

- **Fifteen NIST Interagency/Internal Reports (NISTIR) (10 approved as final and 5 drafts) were issued on a variety of topics, including:**
  A criticality analysis process model, security assurance challenges for container deployment, the cybersecurity framework for federal agencies, a cybersecurity framework manufacturing profile, dramatically reducing software vulnerabilities, code complexity on software analysis, identifying uniformity with entropy and divergence, enhancing resilience of the Internet and communications ecosystem, mobile application vetting services for public safety, lightweight cryptography, privacy engineering and risk management in federal systems, automation support for security control assessments, and small business information security.

- **Formally Launched a Post-Quantum Cryptography (PQC) Standardization Process:**
  The research community has actively responded to the NIST Call for Proposals to

solicit, evaluate, and standardize quantum-resistant public key cryptography (also known as post-quantum cryptography (PQC)) algorithms. Upon the submission deadline, NIST received 82 submissions from 26 countries and 6 continents, among which 69 submissions are considered as complete and proper. The NIST Post-Quantum Cryptography team has worked closely with the submitters and the research community to evaluate and analyze the first-round candidates.

- **Lightweight Cryptography Standards for the Internet of Things (IoT):** The Internet of Things (IoT) tethers heterogeneous "things" together. Some of the "things" are resource constrained. Lightweight cryptography provides critical tools for IoT security. To better understand the need for dedicated lightweight cryptography, the NIST team released a white paper in 2017 to specify two major portfolios for lightweight cryptography primitives. NIST will announce a call for proposals on lightweight cryptography primitives in 2018.

- **A NIST / Industry joint working group continued the development of automated 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 is fully under way, with the full implementation expected in FY 2018. (See: http://csrc.nist.gov/projects/acvt).

- **Published an Initial Public Draft of Special Publication (SP) 800-53, Revision 5:** NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, is a comprehensive set of safeguarding measures that are applicable to all types of computing platforms, including traditional IT systems, cloud and mobile systems, industrial/process control systems, and Internet of Things (IoT) devices. The safeguarding measures in the update to this publication include a full integration of security and privacy controls to protect the operations and assets of organizations and the personal privacy of individuals. Additionally, this update promotes the integration with different risk management and cybersecurity approaches and lexicons, including the Cybersecurity Framework. The Initial Public Comment period resulted in over 3000 comments from over 115 different stakeholders representing the public and private sectors, and academia.

- **Published a Discussion Draft of SP 800-37, Revision 2:** This update to NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, responds to the call by the Defense Science Board, the President's Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, and the Office of Management and Budget Memorandum M-17-25, to develop the next-generation Risk Management Framework (RMF) for systems and organizations. This update provides linkage and communication between the risk management processes and activities at the executive and operational levels of the organization; demonstrates how the Cybersecurity Framework can be implemented using the established NIST risk management processes (i.e., developing a Federal use case); and integrates privacy concepts into the RMF. This discussion draft was issued to inform a public workshop for RMF stakeholders and featured discussions on the risk management methodologies used in various sectors and potential opportunities to improve the RMF.

- **The Cyber Supply Chain Risk Management (C-SCRM) program continued to work with stakeholders to develop and improve FISMA-related guidance on C-SCRM:** C-SCRM controls were significantly modified in a draft of NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, to better align with other guidance. A working group co-chaired by NIST and the Department of Defense

completed a revision of Committee On National Security Systems Directives (CNSSD) Number 505, *Supply Chain Risk Management*, which assigns responsibilities and establishes minimum criteria for the development and deployment of supply chain risk management capabilities for national security systems. Also, NIST collaborated with over 3,000 stakeholders through the Software and Supply Chain Assurance (SSCA) Forum and email list service. The effort, initiated in 2003, is co-led by NIST, the Department of Homeland Security (DHS), the Department of Defense (DOD) and the U.S. General Services Administration (GSA) and provides a venue for government, industry, and academic participants from around the world to discuss cyber supply chain risks, effective practices and mitigation strategies, tools and technologies, and any gaps related to the people, processes, or technologies involved.

- **The goal of the ITL's Usable Security and Privacy project team is to provide guidance for policymakers, system engineers and security professionals so that they can make better decisions that enhance the usability of cybersecurity in their organizations:** The Usable Security and Privacy team contributed usability chapters to SP 800-63, *Digital Identity Guidelines*, marking the first time there were dedicated usability chapters in this flagship NIST security publication. In addition, the usability team also completed a long-term operational phishing evaluation, demonstrating the importance of individual user context in explaining phishing email click decisions.

- **Method developed for efficient automated testing of systems used in Artificial Intelligence (AI) applications:** NIST developed a method of automatically testing and verifying rule-based systems to a high degree of assurance. The method uses a mathematical construct known as a covering array to exhaustively test all components of rules used in many classes of artificial intelligence applications, for a large subset of such applications. The method was incorporated into a proof-of-concept software tool that is freely available.

- **Final Draft of a NIST Special Publication providing guidance on how to securely configure Apple OS X systems:** NIST developed this publication to assist IT professionals in securing Apple OS X 10.10 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.

- **Began the integration of privacy into the Risk Management Framework documents:** A July 2016 update to Office of Management and Budget (OMB) Circular A-130 requires federal agencies to apply the Risk Management Framework to privacy programs - managing privacy risk beyond compliance with privacy laws, regulations and policies. In alignment with this policy, the Privacy Engineering Program in ITL has been working to integrate privacy into the Risk Management Framework documents, providing one unified security and privacy approach – as seen in the initial draft of SP 800-53rev5 and the discussion draft of SP 800-37rev2.

- **Introduced concepts for privacy engineering and risk management as the foundation for the integration of privacy into the Risk Management Framework documents:** The Privacy Engineering Program in ACD published NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*. This publication establishes the basis for a common vocabulary to facilitate better understanding and communication of privacy risk within federal systems, and the effective implementation of privacy principles. It introduces two key components to support the application of privacy engineering and risk management:

privacy engineering objectives and a privacy risk model. These concepts lay the foundation for the integration of privacy into the Risk Management Framework (as seen in the latest revisions of SP 800-53 and SP 800-37).

- **Comprehensive Security Guidance for Virtualized Infrastructures and Contributions to Standards Development:**
  A set of security recommendations for server virtualization were updated in the publication of SP 800-125A, *Security Recommendations for Hypervisor Deployment on Servers*, by including emerging use cases. NIST security guidance for this technology now covers hardware, hypervisor (the core server virtualization software), virtual network and management modules. The active participation of NIST in the editorial team for the International Organization For Standardization/International Electrotechnical Commission (ISO/IEC) 21878, *Security guidelines for design and implementation of virtualized servers*, has advanced the standard from a working draft in October 2016 to a Draft International Standard (DIS) in October 2017. In the area of OS virtualization, the potential solutions for security countermeasures outlined in SP 800-190, *Application Container Security Guide,* were examined, and security assurance requirements for each solution were developed to guide actual security configurations. These security assurance requirements were published in NISTIR 8176, *Security Assurance Requirements for Linux Application Container Deployments,* for the open source Linux platform where application containers are ubiquitously developed and deployed.

- **Established the NIST Cybersecurity Program for the Internet of Things (IoT):**
  ITL created a program for IoT cybersecurity that supports the development and application of standards, guidelines, and related tools to improve IoT cybersecurity. Program establishment included creating an inventory of NIST-wide efforts related to IoT cybersecurity, coordinating among NIST IoT efforts, and convening a team of subject-matter experts to begin drafting guidance on managing IoT cybersecurity and privacy risks.

- **The IoT Program convened cross-sector stakeholders to inform IoT cybersecurity efforts:**
  The IoT Cybersecurity Program coordinated outreach to a range of public and private-sector stakeholders to inform them of NIST's IoT cybersecurity work and collect feedback to inform future work. This included sessions at the Cybersecurity Framework Workshop in 2017, the Industrial Internet Consortium (IIC) quarterly meeting, and planning a colloquium with industry, government, and academic participants.

- **The National Initiative for Cybersecurity Excellence (NICE) program provided numerous communication channels and maintained a visible high-level presence in supporting its mission to the cybersecurity workforce and education fields:**
  The NICE program published three eNewsletters; launched an updated and refreshed the NICE Website to better meet the needs of the NICE Community and visitors; produced 3 new one-page reports and updated the content of three others; produced two ITL Science Day posters; established a LinkedIn presence and hashtag for Tweets from the @NISTCyber twitter account; developed a NICE Multimedia page; participated in seven conference exhibit displays; and hosted ten webinar sessions.

- **The NICE Program also developed and published two NIST publications to support the Cybersecurity Workforce:**
  During FY 2017, the NICE Program published NIST Special Publication 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, and the Draft NIST Interagency Report (NISTIR) 8193, *National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators: Indicators for Performing Work Roles*. The national need for a common lexicon to describe and organize the cybersecurity workforce and the requisite

knowledge, skills, and abilities (KSAs) led to the creation of the NICE Cybersecurity Workforce Framework (NICE Framework). The NICE Framework defines the spectrum of cybersecurity work as well as tasks and for over 50 common Work Roles. While the Work Roles have made the NICE Framework easier to associate with specific positions, they do not provide organizations with guidance on how to determine if a cybersecurity worker can perform a Work Role. NISTIR 8193 is intended to help organizations address this challenge by identifying capability indicators or recommended education, certification, training, experiential learning, and continuous learning that could signal an increased ability to perform a given Work Role.

- **The NICE program provided strategic outreach and engagement with stakeholders throughout FY 2017:**
  The NICE Program increased its outreach efforts to include new academic, industry, and government organizations, including international stakeholders through various meetings and collaborative efforts including the NICE Working Group and NICE Interagency Coordinating Council.

- **Seven NIST National Cybersecurity Center of Excellence (NCCoE) Special Publications (SP) 1800 Series Practice Guides (one revised draft and six new drafts) were issued, providing management, operational, and technical security guidelines in topic areas including:**
  Attribute Based Access Control, Domain Name Systems-Based Email Security, Situational Awareness for the Electric Utilities, Securing Wireless Infusion Pumps in Healthcare Delivery Organizations, Managing Access Rights in the Financial Services Sector, Data Integrity: Recovering from Ransomware and Other Destructive Events, and Derived Personal Identity Verification (PIV) Credentials.

- **The ITL Software Assurance and Quality Program researched and improved how to assess a tool's ability to detect and identify code problems in the Software Assurance Metrics And Tool Evaluation (SAMATE) program:**
  The SAMATE program has three primary components: the Software Assurance Reference Dataset (SARD), the Static Analysis Tool Exposition (SATE), and the Bugs Framework (BF). Mobile applications and test cases used in former Static Analysis Tool Expositions were added to SARD. In 2017, the sixth instance of SATE began.

- **ITL's Computer Forensics Team researched ways to improve the methods for securely acquiring, storing and analyzing digital evidence quickly and efficiently:**
  ITL promoted the efficient and effective use of computer technology to investigate crimes. The project team developed tools for testing computer forensic software, including test criteria and test sets. ITL also maintains the National Software Reference Library (NSRL) – a vast archive of published software applications that is an important resource for both criminal investigators and historians. The NSRL published four releases of the Reference Data Set (RDS) that continues to be the premier software resource. The NSRL was expanded to include mobile apps and to include the profiles obtained from installing and exercising applications.

- **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.

- **In support of FISMA activities, ITL conducted workshops, awareness briefings, webinars, and various outreach to ITL customers:**
  The ITL Cybersecurity Program hosted or provided at least 55 different cybersecurity events throughout FY 2017. These outreach activities were open to the public or for federal agencies. These events covered various Cybersecurity topics – to see the complete list of these events, please see Appendix B at the back of this Annual Report for further details. If a website URL is available for these events – the URLs have been provided.

- **Annual Reports:**
  The ITL Fiscal Year 2017 Cybersecurity Program Annual Report (formerly titled *Computer Security Division Annual Report*) was produced and released as a NIST SP. This report, and previously released CSD annual reports from fiscal years 2003 through 2017, are available on the Computer Security Resource Center (CSRC) website at https://csrc.nist.gov/publications/search?topics-lg=3363%7Cannual+reports

ITL CYBERSECURITY PROGRAM AND PROJECTS

The next section describes accomplishments that were achieved during FY 2017 (covering the time frame October 1, 2016 to September 30, 2017) for the NIST ITL Cybersecurity Program.

(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 INTERNATIONAL IT SECURITY STANDARDS

ITL Involvement with National and International IT Security Standards Work

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); the 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 Mr. Sal Francomacaro serves as the CS1 Vice Chair. CS1 is the U.S. counterpart for the ISO/IEC SC27 committee for IT Security.

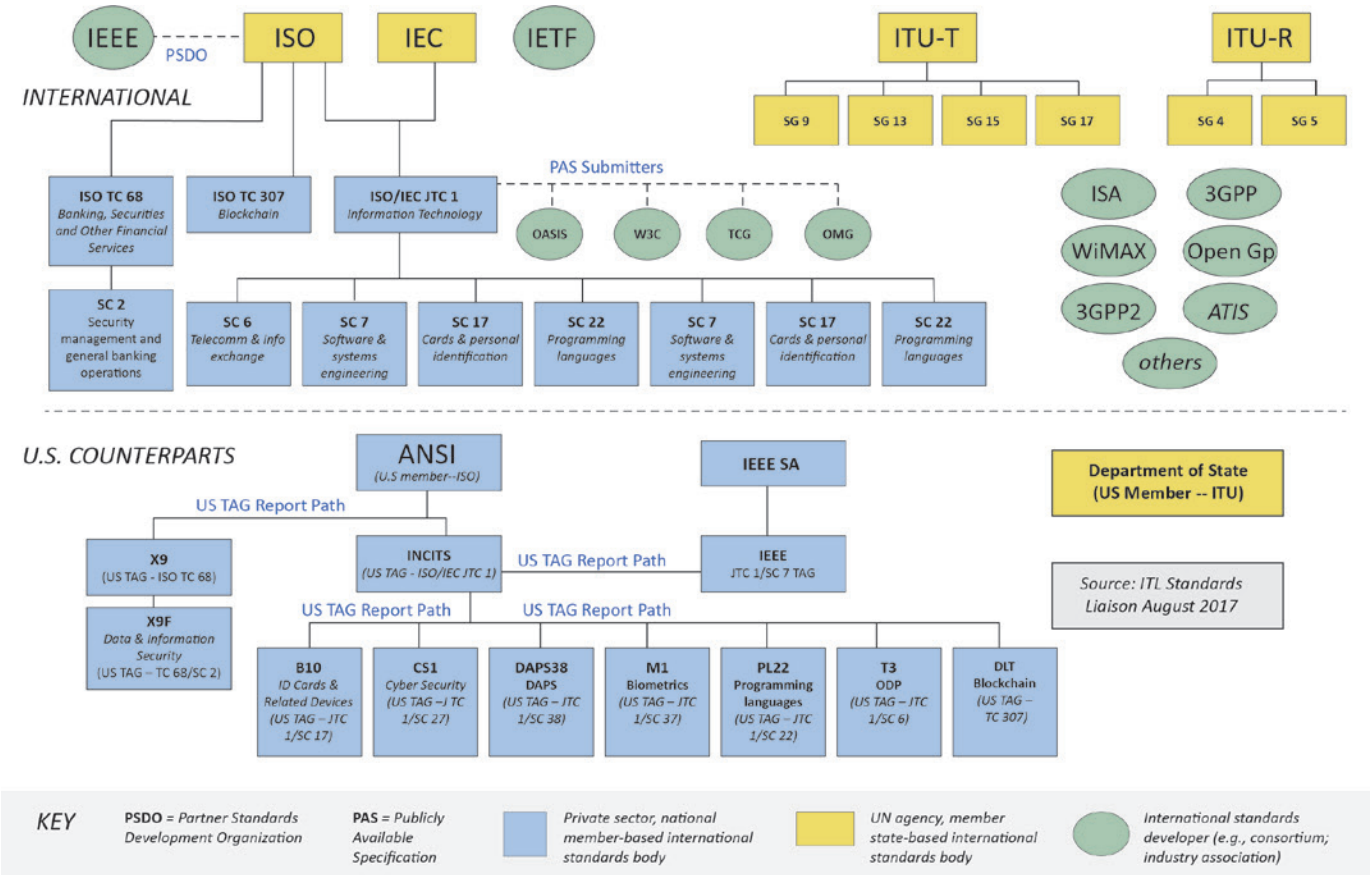


Figure 1: SDOs involved in Cybersecurity

IT Security Techniques Standards – ISO/IEC SC27

The ITL staff actively participate with JTC1/SC27 and its working groups to develop standards for the protection of 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 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.

The 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
salfra@nist.gov

NIST Cybersecurity Framework – International Standardization

The NIST/ITL staff actively participate with JTC1/SC27 and its working groups to support the NIST Cybersecurity Framework International Standardizations strategy.

The main focus for FY 2017 was the development of a Technical Specification based on ISO/IEC 27101 – *Guidelines for developing cybersecurity frameworks*. This Technical Specification (TS) represents the work done by a U.S. group on NIST Cybersecurity Framework and should serve as a guideline for other organizations considering creating a new cybersecurity framework.

The NIST staff was also active in the definition of another ISO Technical Specification: Cybersecurity Overview and Concepts. This TS should target any user concerned with cybersecurity, but is particularly targeted toward decision makers. It should cover, among other things, what cybersecurity IS and IS NOT, how it applies to existing standards, and how it fits in with the other ISO/IEC 27000 series of standards.

The NIST staff will increase participation and effort on these activities during FY 2018.

CONTACT:

Mr. Matt Barrett
(301) 975-6259
matthew.barrett@nist.gov

ISO Standardization of Security Requirements for Cryptographic Modules

ITL is also the principal editor, co-editor, and contributor to many ISO/IEC documents by the ISO/IEC International Organization for Standardization. ITL's contributions to the development of these international standards help to create a strong foundation for the adoption of and migration from currently used national standards. In particular, this adoption promotes international harmonization for the implementation and testing of cryptographic algorithms and modules, while accommodating individual country preferences in the choice of approved security functions.

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 Federal Information Processing Standard (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 second revision of ISO/IEC 19790 was published on August 15, 2012. The second revision of ISO/IEC 24759 was published on January 31, 2014 and the third revision was published March 2017. Both ISO/IEC standards are available through 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.

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 is a chart of the ISO/IEC standards, as explained above, in which CSD has played a part during the development process.

In addition to the aforementioned standards, International Standards ISO/IEC 17825, *Testing methods for the mitigation of non-invasive attack classes against cryptographic modules,* was published on January 15, 2016 and ISO/IEC 18367, *Cryptographic algorithms and security mechanisms conformance testing,* was published on December 15, 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.

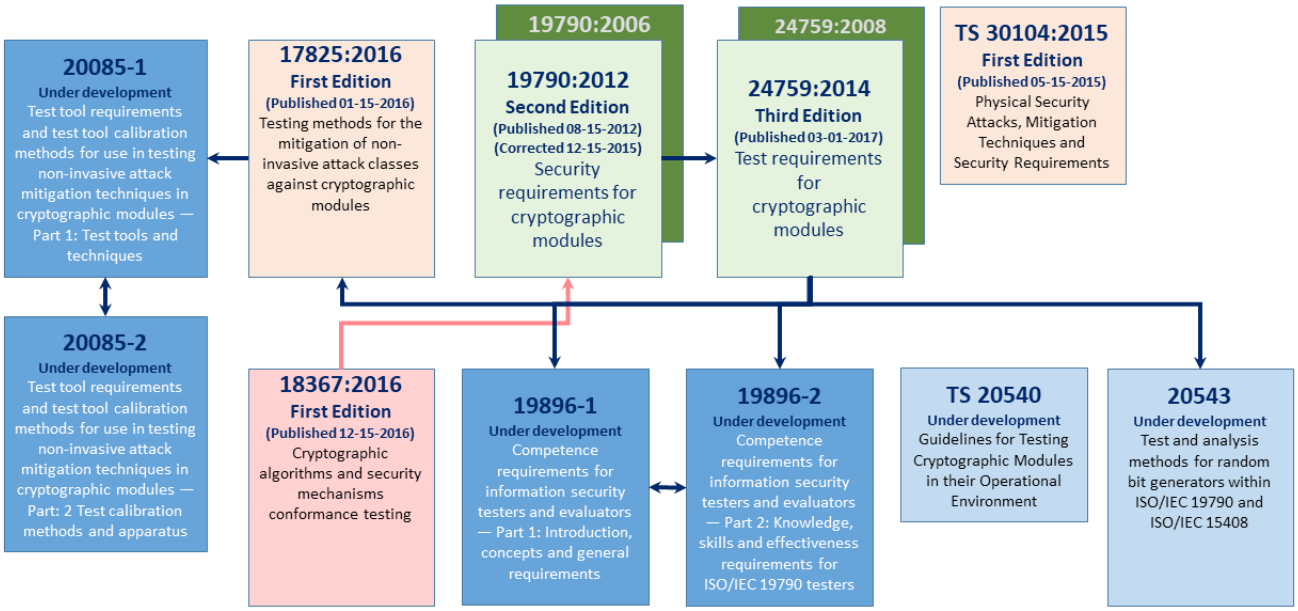


Figure 2: Cryptographic Module Testing – ISO Standards

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.

FOR MORE INFORMATION, SEE:

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

CONTACT:

Mr. Randall J. Easter
(240) 361-8777
randall.easter@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 that are 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 in FY 2018.

CONTACTS:

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

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

Identity Management Devices and Standards

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, the ITL staff:

- Contributed 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;

- Pursued the standardization and harmonization of identity standards that were developed in the U.S.;
- Developed requirements and identified standards gaps for Mobile Driving Licenses;
- Actively participated in the development of a standards for Mobile Driving Licenses;
- Enhanced the Machine-Readable Travel Documents (ePassport) data model to address privacy and security concerns; and
- Contributed to the development of a standard for privacy-enhanced security protocols for secure elements.

The 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 World Wide Web Consortium (W3C). 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). ITL gathered and discussed functional and security requirements for Mobile DLs, and is now developing two models: offline and online. Once these models are fully defined, ITL plans to write technical specifications for each model.

CONTACTS:

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

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

Identity Management International Standardization with ISO/IEC SC27

During FY 2017, NIST ACD's Trusted Identities Group (TIG) collaborated with representatives from the United Kingdom (U.K.) Cabinet Office and the Canadian Treasury Board to identify commonalities and work to align the digital identity standards and requirements among the respective national digital identity programs, particularly SP 800-63-3 for the U.S. and the U.K. Good Practice Guides (GPG). The goal in these efforts is to promote a vibrant market of internationally viable identity services and advance the secure exchange of digital identities while protecting the privacy of the subjects of those identities for cross-border transactions and mutual recognition. While primarily focused on developing a framework that would facilitate the establishment of a common set of requirements and standards across the three national programs, there was increasing interest from other national programs and industry in the work products and methodologies developed by this collaborative work. As a result, the group provided this work to the international community as a series of aligned joint contributions for international standardization.

The TIG contributions, in collaboration with their British and Canadian partners, were focused on establishing a synchronized core set of international identity management standards within the scope of the activities of ISO/IEC JTC 1/SC 27/WG 5, which oversees the development of international standards for identity management and privacy. The team provided contributions to synchronize and align the following ISO/IEC standards with the U.K., Canadian, and U.S. harmonization work:

- **ISO/IEC 29115 Information Technology — Security techniques — Entity authentication assurance framework** – a major revision is required to align with SP 800-63 B and GPG 44;
- **ISO/IEC 29003 Information technology — Security techniques — Identity proofing;**
- **ISO 31000 Risk management framework applied to identity-related risk,** a new work project for a new international standard that will be aligned with the risk management section of NIST SP 800-63-3;
- **Identity related standards landscape,** a new work project to establish a clear and aligned landscape for ISO/IEC identity standards and administrative processes and to establish rules for how the development and maintenance of an aligned set of identity management standards could be coordinated and managed within ISO/IEC WG5; and
- **Identity assurance framework,** a new work project for a new international standard that will be aligned with the identity assurance components of SP 800-63A and the U.K. GPG 45.

CONTACT:

Mr. David Temoshok
(202) 482-5475
david.temoshok@nist.gov

Blockchains

During FY 2017, NIST participated in standards activities exploring blockchain technologies, architectures, and use cases. These included participation in a new blockchain study group sponsored by the American Standards Committee X9, the financial services committee of the American National Standards Institute (ANSI), and continued work in the International Standards Organization (ISO) Technical Committee (TC) for Blockchains and Distributed Ledger Technologies (ISO/TC 307). Established in 2016, the initial objectives of ISO/TC 307 include defining key terms and concepts, exploring reference architectures, investigating use cases, and identifying identity and privacy implications within blockchain technologies and architectures. NIST has been participating in these activities via the national mirror committee within the InterNational Committee for Information Technology Standards (INCITS). ISO/TC 307 will meet in November 2017, where the reports on these topics will be reviewed and new work will be established.

CONTACTS:

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

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

Internet of Things (IoT)

NIST/ITL has contributed to standardization activities for the IoT architecture and vocabulary during FY 2017 in three primary areas:

- The Industrial Internet Consortium (IIC);
- ISO/IEC SC41, *Internet of Things and related technologies*; and
- IEEE P2413, *Standard for an Architectural Framework for the Internet of Things (IoT)*.

Focus was on the architecture, vocabulary, and recently, edge computing. In addition to working on standards related to these areas, NIST staff member Eric Simmon is the chair of the IIC commenting working group for reviewing the IEEE p2413 draft standard and is the liaison between ISO/IEC SC41-ISO/IEC SC38 (cloud computing).

The NIST staff has also participated to the activities in ISO/IEC SC27 relative to IoT Security. This activity will be further developed during FY 2018.

CONTACTS:

Mr. Eric Simmon
(301) 975-3956
eric.simmon@nist.gov

Ms. Katerina Megas
(202) 441-1147
katerina.megas@nist.gov

Cloud Computing Standards Developed Within ISO/IEC JTC 1

ITL is actively engaged with several key players in the Federal Government which look broadly at questions of IT standards, how to influence them, and

how to use them. These participants include the Office of Management and Budget (OMB) E-Gov Office and Office of Information and Regulatory Affairs, the federal Chief Information Officers (CIO) Council, the Interagency Council on Standards Policy (ICSP), and the General Services Administration (GSA) Office of Government-wide Policy. Our goal in chairing the Standards Working Group is to solicit requirements from federal agencies, find the appropriate voluntary standards committee that is addressing these requirements and encourage participation to ensure the government requirements are being adequately met. Where standards are needed, ITL works closely with U.S. industry, standards development organizations, other government agencies, and leaders in the global standards community to develop standards that will support secure cloud computing.

ITL participation helps to ensure the alignment of NIST standards with those of ISO/IEC JTC 1 sub-committees, such as SC 27 IT Security techniques, SC 38 Cloud Computing and Distributed Platforms, and their U.S. counterparts, ANSI/ INCITS Cyber Security 1 (CS 1) and Cloud 38. The large number of standards being developed in SC 27 covering areas such as security, cryptography, privacy, supply chain, personally identifiable information (PII) processing or virtualization security, harmonize with many cloud computing standards being developed by these subcommittees.

The focus of implementing cloud computing is even more critical since the White House released an IT Modernization Report in September 2017 that includes recommendations for agencies to take steps to secure and modernize federal IT networks. Those steps for modernizing and consolidating networks point to cloud computing, modernization of government-hosted applications, and better security for legacy systems. Federal modernization efforts, such as those connected with the Modernizing Government Technology Act, may further enable agencies to accelerate investments in cloud and other new technologies.

Ms. Annie Sokol is a member of ITL's Cloud Computing team and is 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 SC 38. Ms. Sokol is the co-editor of ISO/IEC 19941, *Information technology–Cloud computing–Interoperability and portability,* which is expected to be published by the end of 2017. The document is intended to establish a common understanding of cloud computing interoperability and portability. Both interoperability and portability offer more choices to cloud users by limiting the effects of being locked-in to any cloud service or cloud service provider. ISO/IEC 19941 joins many published cloud computing standards that were developed from NIST publications, such as:

- ISO/IEC 17788, *Information technology -- Cloud computing -- Overview and vocabulary*;
- ISO/IEC 17789, *Information technology -- Cloud computing -- Reference architecture;* and,
- ISO/IEC 19086, *Information technology -- Cloud computing -- Service level agreement (SLA) framework.*

CONTACT:

Ms. Annie Sokol
(301) 975-2006
annie.sokol@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 of 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—identify, assess, and manage cybersecurity-related risk while protecting business confidentiality, individual privacy, and civil liberties.

In FY 2017, NIST continued to work with a diverse stakeholder community to support the use and understanding of the Cybersecurity Framework. This process included:

- Publication of a draft Framework 1.1 to clarify, refine, and enhance the Cybersecurity Framework, drawing upon comments received from a public review process launched in January 2017;
- Conducting a public workshop at NIST in Gaithersburg, MD to gather input about the current use of the Framework and feedback regarding the initial public draft;
- Releasing the 1.0 version of the Baldrige Cybersecurity Excellence Builder, a self-assessment tool to help organizations better understand the effectiveness of their cybersecurity risk-management efforts;
- Updates to the Framework website with a catalog of industry resources, upcoming NIST speaking events, and an extensive frequently-asked-question knowledge base;
- Provision of outreach for small- and medium-sized businesses (SMBs), including guidance provided by the Applied Cybersecurity Division (ACD) in NIST Interagency Report (NISTIR) 7621 Rev. 1, *Small Business Information Security: The Fundamentals*;
- 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;
- 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. NIST has strengthened its collaboration with critical infrastructure owners and operators, industry leaders, government partners, and other stakeholders—building on previous years' interactions that were crucial to the Framework's development.

In May 2017, Executive Order 13800 was released, directing federal agency heads to use the Framework to manage agencies' cybersecurity risk. NIST released draft NISTIR 8170, *The Cybersecurity Framework: Implementation Guidance for Federal Agencies*, to provide information on how Federal agencies can use the Cybersecurity Framework—and in particular, how the Risk Management Framework and Cybersecurity Framework work together to help agencies develop, implement, and continuously improve their information security programs.

In FY 2018, NIST 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. Version 1.1 of the Framework is expected to be published, and NIST will continue to identify ways for the Framework to contribute to risk management initiatives.

FOR MORE INFORMATION, SEE:

https://www.nist.gov/cyberframework

CONTACTS:

Mr. Matt Barrett
(301) 975-6259
matthew.barrett@nist.gov

Mr. Jeff Marron
(301) 975-3846
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 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 https://csrc.nist.gov/Projects/Risk-Management).

During FY 2017, 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), 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 continued to work 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 as well as on developing guidance and a security controls overlay to protect federal high value assets.

In FY 2017, the ITL FISMA Team worked on the following initiatives:

- **System Security Engineering Initiative:** The final version of Special Publication (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 is 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, beginning in 2018. 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 continued on SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*. The initial public draft was published after collaboration with a federal interagency working group, the OMB, NIST, other agency privacy professionals, and 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 FISMA Team, in conjunction with the same group of collaborators, also published a discussion draft of SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations*. SP 800-37 Revision 2 provides a closer link between risk

management processes and activities at the executive level of the organization, with risk management activities at the system and operational level; institutionalizes enterprise-wide risk management preparatory activities to facilitate a more efficient and cost-effective execution of the Risk Management Framework at the system and operational level; demonstrates how the Cybersecurity Framework can be implemented using the established Risk Management Framework processes; and integrates privacy concepts into the Risk Management Framework. The implementation of SP 800-53, SP 800-37, 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, conducted outreach activities with academic institutions, provided information on NIST's security standards and guidelines, and explored 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 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 CNSS working groups.

In FY 2017, the FISMA Team completed the following activities:

- Published the final version of SP 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems;*
- Published the initial public draft of SP 800-53 Revision 5, *Security and Privacy Controls for Systems and Organizations;*
- Published the discussion draft of SP 800-37 Revision 2, *Risk Management Framework for Federal Information Systems: A System Life Cycle Approach for Security and Privacy;*
- Published the final version 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 final versions of NIST Interagency Report (NISTIR) 8011, *Automation Support for Ongoing Assessments, Volume 1 - Overview,* and *Volume 2 - Hardware Asset Management,* and adjudicated public comments in partnership with DHS*;*
- Published the final version of *An Introduction to Information Security;*
- Continued 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 (NARA);
- Continued the development of the initial public draft of SP 800-18 Revision 2, *Guide for Developing System Security and Privacy Plans;* and
- Continued the development of the initial public draft of SP 800-47 Revision 1, *Information Exchange and System Connections.*

In FY 2018, the FISMA Team intends to:

- Continue work on SP 800-160 companion publications;
- Finalize and publish the final version of SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations;*
- Finalize and publish the final version of SP 800-37 Revision 2, *Risk Management Framework for Federal Information Systems: A System Life Cycle Approach for Security and Privacy;*
- Complete the development of and *operationalize* the 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;
- Publish the initial public draft and final version of SP 800-53A, *Assessing Security and Privacy Controls in Information Systems and Organizations;*
- Publish the initial public draft and final version of SP 800-171A, *Assessing Security Controls in Nonfederal Systems*;
- Continue the development of SP 800-18 Revision 2, *Guide for Developing System Security and Privacy Plans;*
- Finalize and publish SP 800-47 Revision 1, *Information Exchange and System Connections;*
- Update the RMF online course to Hypertext Markup Language version 5 (HTML5) and verify consistency with SP 800-37 Revision 2;
- 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:

https://csrc.nist.gov/projects/risk-management

CONTACTS:

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

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

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

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

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

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

Editor's Note: Ms. Peggy Himes worked on this project until her recent retirement.

Privacy Engineering Program

The NIST 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.

In FY 2017, the PEP focused on 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). Many of the PEP's efforts in FY 2017 were fueled by the OMB's July 2016 update to Circular A-130, which emphasized federal agencies' responsibilities to manage privacy risk, not just compliance risk, and now requires them to apply the NIST Risk Management Framework to their privacy programs.

Advancement of Privacy Engineering and Risk Management

In January 2017, the PEP reached a major milestone in advancing the development of privacy engineering and risk management processes with the finalization of NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems* (see https://doi.org/10.6028/NIST.IR.8062). NISTIR 8062 introduces the concept of applying systems engineering practices to privacy and provides a new model for conducting privacy risk assessments on federal systems. It also presents the PEP's initial roadmap (See Figure 3) for guidance development to help agencies more effectively meet new obligations under the revised Circular A-130.

In FY 2017, the PEP team collaborated with internal and external partners to successfully integrate privacy requirements and considerations into SP 800-63-3, *Digital Identity Guidelines*. The PEP team also collaborated to integrate privacy into the draft revisions of SPs 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, and 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations*, building the foundation of making privacy and security equal

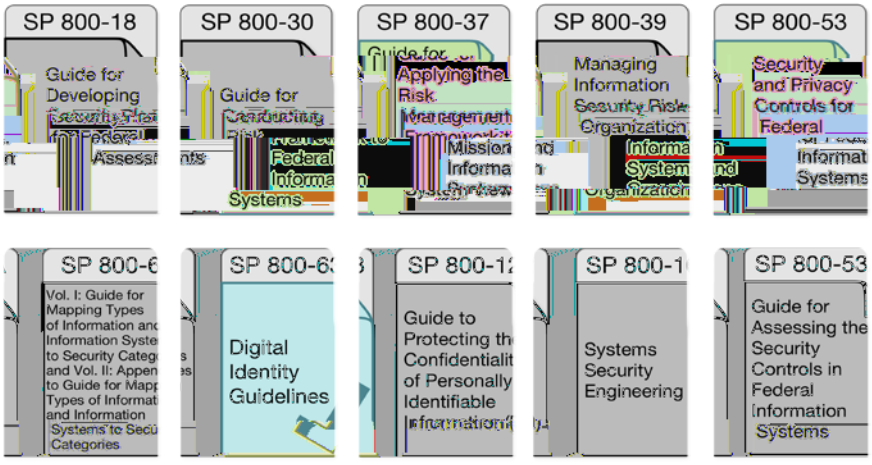


Figure 3: PEP guidance roadmap for integrating privacy risk management into NIST SPs, featuring integrations underway during FY 2017 (highlighted in green).

quality attributes in trustworthy systems. The PEP team also contributed privacy concepts to the Trusted Identities Group (TIG) measurement science effort, draft NISTIR 8112, *Attribute Metadata*.

The PEP team also contributed to ongoing standards and framework development efforts in the International Organization for Standardization (ISO), Institute of Electrical and Electronics Engineers (IEEE), and the Fast Identity Online (FIDO) Alliance. Specifically, the PEP team worked on ISO/IEC 27552, which is a privacy-focused sector-specific extension of the information security-focused ISO/IEC 27001, and ISO/IEC 27550, a technical report on privacy engineering. The PEP team also supported the development of IEEE P7002, an effort in its early stages that also addresses privacy engineering. The PEP team also engaged with FIDO to help develop privacy-enhancing authentication specifications.

Continuing the ongoing series of NIST workshops on privacy engineering and risk management, building off the concepts introduced in NISTIR 8062, the PEP team hosted the June 2017 workshop, "Privacy Risk Assessment: A Prerequisite for Privacy Risk Management" (see https://www.nist.gov/news-events/events/2017/06/privacy-risk-assessment-prerequisite-privacy-risk-management). Feedback received included the need for further integration of privacy into risk management and security guidance, a privacy-specific risk assessment model, and a toolset to manage privacy risk. These takeaways aligned well with the PEP team's ongoing efforts and goals for future work.

In support of a privacy-specific risk assessment tool, the PEP team continued socializing the use of its Privacy Risk Assessment Methodology (PRAM) inside and outside the Federal Government. As of FY 2017, more than 30 public- and private-sector organizations have used or are using the PRAM, including participants in NIST's trusted identities pilots and a few federal agencies.

The PEP team also collaborated on projects at the National Cybersecurity Center of Excellence (NCCoE), including the Privacy-Enhancing Identity Federation building block, which demonstrates the use of the NIST privacy engineering objectives (see https://nccoe.nist.gov/projects/building-blocks/privacy-enhanced-identity-brokers).

NIST Leadership in Privacy

The PEP team built upon NIST's leadership role in privacy by serving in leadership positions and contributing to privacy expertise organizations across the public and private sectors. These leadership positions included: the chair of the Federal Privacy Council's Risk Management Task Force and co-chair of the Networking and Information Technology Research and Development (NITRD) Program's Privacy Research and Development (R&D) Interagency Working Group. The PEP team also participated in the Internet Policy Task Force's Privacy Working Group, the FIDO Alliance's Privacy and Public Policy Working Group, and the Identity Ecosystem Steering Group.

Looking Forward

In FY 2018, the PEP team will continue developing privacy risk management guidance for agencies, including finalizing SP 800-53 Revision 5, and SP 800-37 Revision 2. The PEP team will also collaborate with internal and external stakeholders to kick off the integration of privacy guidance into SP 800-53A Revision 5, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations,* and implement the provisions of other documents laid out in the guidance roadmap. The PEP team will continue supporting the development of international standards focused on privacy engineering and risk management.

The PEP team will place a greater focus on its goal of advancing the deployment of privacy-enhancing technologies. The PEP team has already begun exploring whether stakeholders see a need for an online space where collaborators can discuss, learn about, and improve upon tools, solutions, and processes that support privacy engineering and risk management. The PEP team will also explore the management of privacy risk in leading-edge domains, such as the internet of things (IoT) and artificial intelligence (AI). Specifically, the PEP team will collaborate with NIST's Cybersecurity for the IoT program to tackle IoT-specific privacy challenges through workshops and guidance.

The PEP team will continue to seek leadership opportunities in public- and private-sector organizations to strengthen NIST's position as a leader in privacy. Finally, the PEP team will continue working with a

variety of organizations to manage privacy risk using the PRAM, such as using it in the NCCoE's Mobile Device Security building block.

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

Ms. Katie Boeckl
(240) 753-9674
kaitlin.boeckl@nist.gov

Cyber Supply Chain Risk Management (C-SCRM)

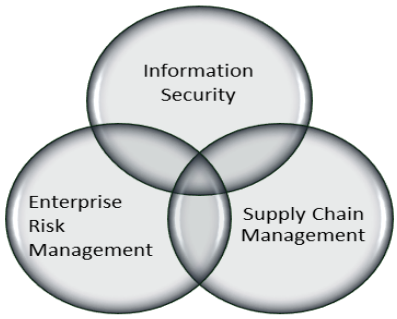


Figure 4: C-SCRM Disciplines

Over the last several years, providing information and operational technology (IT/OT) for a supply chain has evolved into a complex, globally distributed, dynamic ecosystem enabling the development of highly refined, sophisticated, cost-effective, and reusable solutions. This ecosystem is composed of assorted entities with multiple tiers of outsourcing, global distribution routes, diverse technologies, and varying laws, policies, procedures, and practices, all of which interact throughout the life cycle of a system. Factors that allow for low-cost products, rapid innovation, and other benefits also increase the risk that the supply chain may be compromised in a way that results in risks to the end user and reduce the overall competitiveness of U.S. companies.

Cyber Supply Chain Risk Management (C-SCRM) lies at the intersection of information security, supply chain management, and enterprise risk management (Figure 4); it is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/OT product and service supply chains. C-SCRM 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 IT/OT product or service at any stage. These cyber supply chain risks may include the use of counterfeits, unauthorized production, tampering, theft, and insertion of malicious software and hardware, as well as poor manufacturing and development practices. As shown in Figure 5, C-SCRM is concerned with and involves a range of subjects, including safety, integrity, quality, reliability, and others, all within an overall environment of awareness.

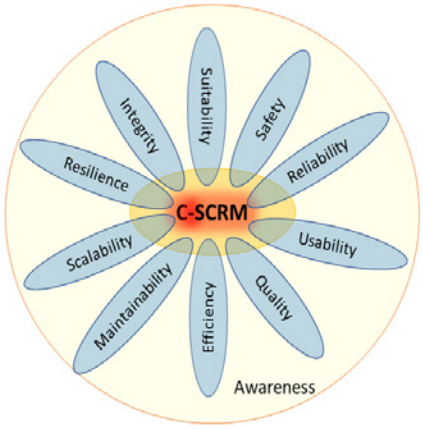


Figure 5: C-SCRM Aspects

In FY 2017, NIST drafted NISTIR 8179, *Criticality Analysis Process Model,* a method for identifying and prioritizing IT/OT systems and components. This model is intended to increase an organization's ability to make cost-effective risk decisions by determining the systems and components that have the most impact on the organization and that would potentially cause the most harm if compromised. Figure 6 shows an overview of the model, which includes separate analyses at the program, system, and component level, and then a trace-back exercise to complete the analysis. NIST will finalize this publication in FY 2018 and will begin to research and write guidance that builds on this model to identify critical suppliers and service providers.

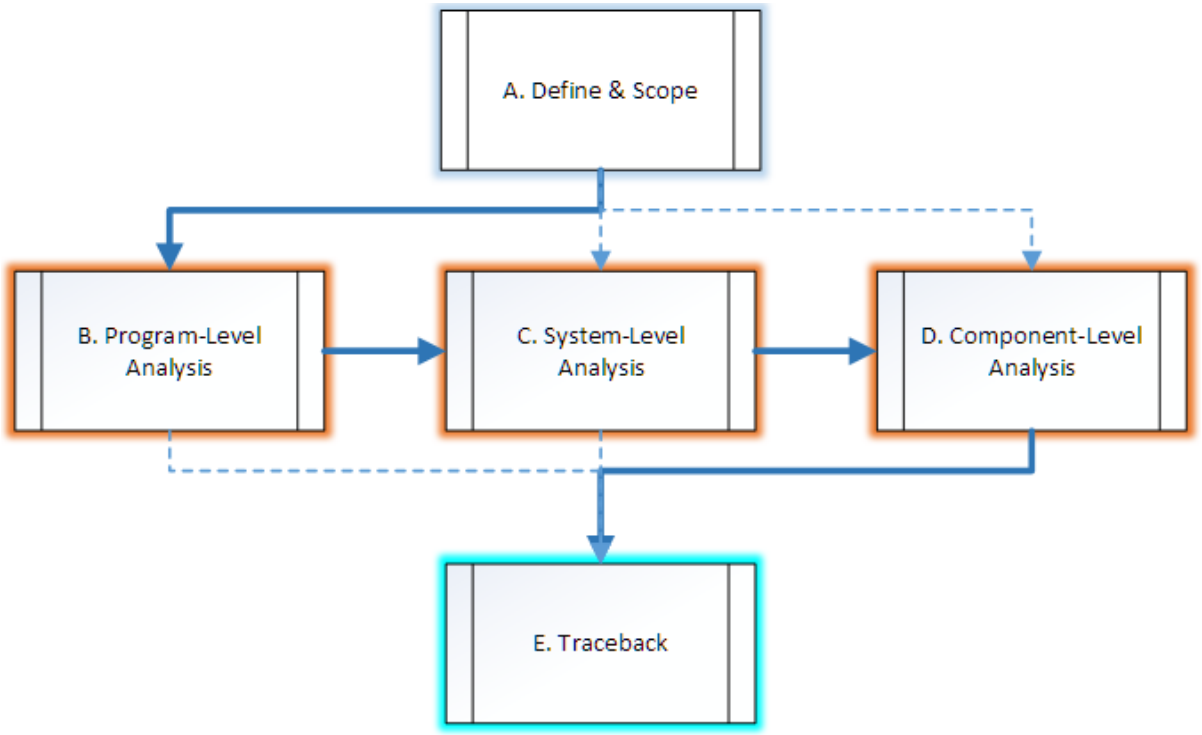


Figure 6: Criticality Analysis Process Overview

During 2017, NIST continued to research the state of C-SCRM in both the public and private sectors, related standards and initiatives, effective practices, and metrics. NIST joined with the GSA and the University of Maryland under a contract and grant awarded in FY 2016 to conduct cyber analytics research on the effectiveness of various risk management practices. The effort neared conclusion in FY 2017 and found correlations between certain practices and publicly disclosed data breaches. A report on the research will be published in FY 2018.

Similarly, NIST began research in FY 2017 to identify metrics that are currently used in organizations to measure information security risks. This research included a review of over 200 published standards, academic papers, organizational white-papers, and other documents and interviews with a dozen industry experts on the state of metrics in this field. The research will be continued and published in FY 2018.

NIST continued to co-chair a working group with the DoD to revise CNSSD 505, *Supply Chain Risk Management*, which assigns responsibilities and establishes minimum criteria for the development and deployment of supply chain risk management capabilities for national security systems. In FY 2017, the group completed the revision of CNSSD 505 and developed a self-assessment tool to help agencies measure their capabilities and compare those capabilities to those of other agencies.

NIST also sponsored 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 three to four times a year and cover a variety of subjects of interest to attendees (see the website at https://csrc.nist.gov/scrm/ssca).

NIST began working in FY 2017 to integrate C-SCRM into existing risk management programs and processes. The draft Cybersecurity Framework v1.1 and Draft SP 800-53 Revision 5 were both updated to better include up-to-date C-SCRM guidance. In FY 2018, NIST will continue this work by including or updating existing C-SCRM concepts in other publications as they are developed.

In FY 2018, NIST 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. NIST will:

- Update SP 800-161 based on the final publication of SP 800-53 Revision 5,
- Continue developing industry supply chain risk management case studies,
- Develop a draft NISTIR on SCRM "principles",
- Develop a NISTIR on Supply Chain Interdependency Analysis, and
- Continue research and work on metrics and cyber risk analytics.

FOR MORE INFORMATION, SEE:

https://scrm.nist.gov

CONTACTS:

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

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

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

Software and Supply Chain Assurance Forum

Cyber supply chain risk management (hardware and software assurance and assured services) has become a topic of core strategic concern for business and government leaders worldwide and is an essential component of an enterprise risk management strategy. The Software and Supply Chain Assurance (SSCA) Forum provides a venue for government, industry, and academic participants from around the world to share their knowledge and expertise regarding cyber supply chain risks, effective practices and mitigation strategies, tools and technologies, and any gaps related to the people, processes, or technologies involved.

The effort, initiated in 2003, is co-led by NIST, DHS, DoD and GSA, and serves approximately 3,000 stakeholders. Participants represent a diverse group of career professionals, including government officials, chief information security officers, those in academia with cybersecurity and supply chain specialties, system administrators, engineers, consultants, vendors, software developers, managers, analysts, specialists in IT and cybersecurity, and many more fields. The SSCA Forum meets two to three times per year and is free and open to all interested participants, both nationally and internationally.

While the general intent is to share information, the SSCA Forum also offers government and private-sector participants an opportunity to openly collaborate by presenting and receiving feedback on current and potential future work. Most events are two to three days long and contain a mixture of discussion and presentation. To encourage open interaction, SSCA Forum meetings operate under the Chatham House Rule, meaning "*participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed*," though most speakers allow NIST to post their presentations.

The SSCA Forum also maintains an extensive email subscription service. To receive information about upcoming meetings and related publications and activities, please sign up for the SSCA Forum mailing list, operated by NIST, by sending a blank email to sw.assurance-join@nist.gov.

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management/SSCA

CONTACTS:

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

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

BioCTS

In early 2017, a suite of BioCTS applications was released to support user-defined requirements and profiles for ANSI/NIST-ITL (AN-ITL) specifications. These applications make use of configuration files to dynamically generate parsing rules and conformance requirements for nearly any version or profile of the AN-ITL standard. The configuration files utilize an Extensible Markup Language (XML)-based format called ANSI/NIST-ITL Machine Readable Tables (MRTs) (see Figure 7 for an example output). The BioCTS AN-ITL applications that use MRTs are collectively referred to as BioCTS AN MRT.

The development of BioCTS applications traditionally relied on the publication of Conformance Testing Methodology (CTM) documentation, which specified the test assertions required to assess conformance to requirements found in the related biometric standard. Manual software development was then required to code each of the assertions listed in the CTM documentation. This process required a large amount of development time after the publication of the standard and related CTM, and often resulted in long delays in the release of conformance tools. This approach also defined conformance tests statically, meaning that:

- End users with domain-specific requirements or user-defined fields were not able to modify the conformance tests or parsing rules.
- Any modification to the base standard requirements or subsequent revision of the standard required a new release of BioCTS applications.

To alleviate these issues, the new version of BioCTS was designed to allow a modification of test assertions and parsing rules. This approach required a configuration file to specify requirements and allow the software to respond to the needs of the end user.

BioCTS AN MRT had two releases in FY 2017. The first release included a command line interface (CLI) as well as a graphical user interface (GUI). It supported Level-1 testing, file format testing that checks for the allowed content, length, and value for five different standards and profiles specified within the AN MRTs. Since the MRT files can be combined to support multiple standards, updates and profiles, BioCTS AN MRT was designed to allow users to test against multiple standards during a single test.

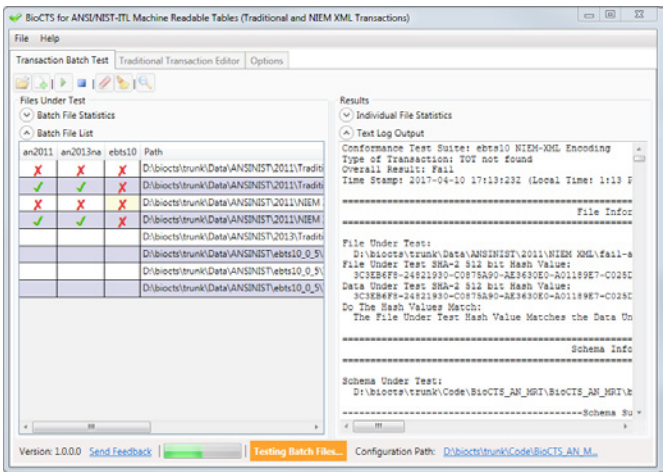


Figure 7 - BioCTS AN MRT Testing Multiple Standards Within Single Test

The second release included further refinements of the existing tools, and expanded the testing capabilities to include Level-2 testing, or the testing of inter-field as well as inter-record relationships, checking data between two or more related data fields. The current release of BioCTS AN MRT supports all Level-1 and Level-2 tests defined by the MRTs.

Work on BioCTS AN MRT continued through FY 2017, and an additional release that supports expanded character sets, as well as additional enhancements, is expected to be released in FY 2018.

FOR MORE INFORMATION, SEE:

BioCTS - Biometric Conformance Test Tool Homepage:

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

BioCTS AN MRT:

https://www.nist.gov/itl/csd/biometrics/biocts-machine-readable-tables

BioCTS AN MRT Changelog:

https://www.nist.gov/file/384611

BioCTS AN MRT User Guide:

https://www.nist.gov/file/384606

CONTACT:

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

CYBERSECURITY APPLICATIONS

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.

NIST and the EAC established a set of public working groups to inform the development of a new version of the Volunary Voting Systems Guidelines (VVSG). The NIST and EAC goals are to accelerate the development and adoption of the VVSG by leading these working groups in close consultation with election officials, voting system manufacturers, standards bodies, academic researchers, and other members of the public. These working groups focus on multiple voting system technology areas, including accessibility, usability, interoperability, security, testing and certification.

The cybersecurity public working group designed principles and guidelines to form the basis for the security requirements in the new version of the VVSG. Although 15 principles exist, the security-related principles include auditability, ballot secrecy, physical security, access control, system integrity, detection and monitoring, and data protection. Many of these principles are already included in previous iterations of the federal standards, whereas others are new areas of focus (e.g., system integrity). These principles and guidelines were presented to, and adopted by, the Technical Guidelines and Development Committee (TGDC).

In FY 2018, NIST will continue leading the public working groups to inform the development of voting system requirements based on the principles and guidelines. Additionally, test assertions will be developed to improve the quality and consistency of testing activities by accredited voting system test laboratories (VSTLs).

FOR MORE INFORMATION, SEE:

https://vote.nist.gov

CONTACTS:

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

Ms. Gema Howell
(301) 975-6299
gema.howell@nist.gov

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

Nationwide Public Safety Broadband Network (NPSBN) Cybersecurity

Source: https://www.pscr.gov/

In February 2012, Congress passed the Middle Class Tax Relief and Job Creation Act. One portion of this legislation calls for the establishment of a nationwide, interoperable public-safety broadband network based on the 3rd Generation Partnership Project's (3GPP) Long Term Evolution (LTE) technology. The network will be deployed and operated by the First Responder Network Authority (FirstNet). The planned 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 https://www.ntia.doc.gov/category/public-safety). NIST is directed to conduct research and development that supports the acceleration and advancement of the nationwide network.

In FY 2017, CSD, ACD, and the NCCoE continued to support the joint National Telecommunications and Information Administration (NTIA) and NIST Public Safety Communications Research (PSCR) program (see https://www.pscr.gov) with efforts in public-safety mobile-application security, identity management, data and application isolation technologies, wearable devices, and broadband standards. The PSCR's Annual Public Safety Broadband Stakeholder Conference, held in June 2017, continued to be a valuable venue for ITL to provide updates on each of our ongoing projects. The conference also provided a venue to directly interface with the public safety and first responder communities.

The mobile devices that will operate on the NPSBN will be utilized in unique ways when compared to their public counterparts. The same device(s) will likely be shared between public safety officials as each individual goes on and off duty. Furthermore, there will be a need for flexible distribution and credentialing of devices and users in situations where multiple public safety organizations are called into action. To facilitate these needs NIST, through the NCCoE, piloted a proof-of-concept single sign on (SSO) for mobile applications on iOS and Android.

Due to the vital nature of first responder activities, the mobile applications that will serve public safety in their mission will require more scrutiny when evaluated for software bugs and vulnerabilities than applications targeted at the public. In FY 2017, NIST continued to expand its expertise in mobile application vetting tools and practices. In addition to publishing NISTIR 8136, *An Overview of Mobile Application Vetting Services for Public Safety*, ACD, in conjunction with NIST Software and System's Division (SSD), expanded the Static Analysis Tool Exposition (SATE) to include mobile application analysis for the first time. This exposition seeks to improve methods for measuring the effectiveness of mobile application vetting tools.

ITL continued to participate 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). NIST also broadened its participation in 3GPP's 5th Generation Mobile Networks (5G). In addition, researchers broadened their scope within the Internet Engineering Task Force (IETF) to include efforts related to public safety.

In FY 2018, CSD and ACD will continue to strengthen NIST's relationship with both public safety and commercial telecom stakeholders. Work concerning mobile application vetting and cyber security will continue to evolve as NIST refines both its methods for tool evaluation as well as its corpus of test cases used in those evaluations. PSCR is working diligently to fund grants and prize challenges to both solve current problems and fill future gaps in public safety broadband technology. In FY 2018, ITL will also take on a crucial role in this work by providing cybersecurity expertise and guidance in the administration of these awards.

CONTACTS:

Mr. Michael Ogata
(301) 975-6993
michael.ogata@nist.gov

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

Cybersecurity for Industrial Control Systems

NIST's Industrial Control System (ICS) cybersecurity effort is focused on providing guidance and insights into the domain of securing connected physical systems. ACD is supporting the NIST Engineering Laboratory's (EL) effort to develop and implement guidance aimed at effectively securing ICS, initially focusing on Smart Manufacturing Environments. Using an ICS cybersecurity testbed, a portion of which is shown in Figure 8, NIST will measure the network and operational 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 International Society of Automation (ISA) standard ISA/IEC-62443 and SP 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security* (see https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf).

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 potential vulnerabilities and increased the potential risk to manufacturing operations. While these manufacturing systems become smarter and increasingly connected, providing a tremendous increase in value and efficiency, they also present a new challenge: "How is cybersecurity effectively applied to this connected domain?"

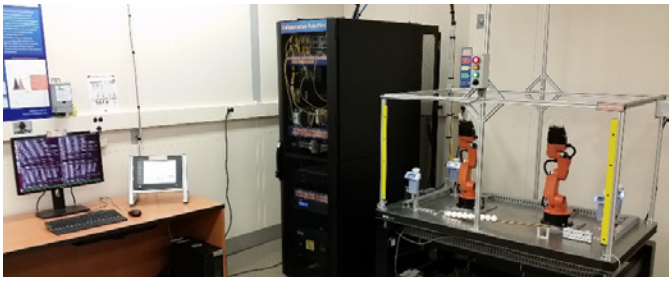


Figure 8: Collaborative robotics portion of the ICS cybersecurity testbed

The ICS cybersecurity team has used existing standards, in conjunction with the NIST *Framework for Improving Critical Infrastructure Cybersecurity*, 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 that is aligned with manufacturing sector goals and industry best practices. The profile tailors existing cybersecurity control language to be more aligned with operational technology environments, focusing on desired cybersecurity outcomes to identify opportunities for improving the current cybersecurity posture of a manufacturing system. Through a session during the 2016 Cybersecurity Framework Workshop and two public comment periods, the team solicited feedback from industry partners to help solidify the content in the profile. The *Cybersecurity Framework Manufacturing Profile* was published as NISTIR 8183 (see https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf).

In 2018, NIST will continue the process of applying the guidance presented in the Manufacturing Profile by implementing the recommended cybersecurity controls within the ICS cybersecurity testbed. This application of cybersecurity controls in an ICS environment will enable the measuring and understanding of the network and operational performance impacts that cybersecurity protections have on these systems. In addition to providing performance data, this project will produce documentation relating to the implementation intricacies and special requirements presented by these non-traditional environments.

FOR MORE INFORMATION, SEE:

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

CONTACTS:

Mr. Jeffrey Cichonski
(301) 975-3293
jeffrey.cichonski@nist.gov

Mr. Keith Stouffer (EL)
(301) 975-3877
keith.stouffer@nist.gov

Smart Grid Cybersecurity

In December 2007, Congress passed the Energy Independence and Security Act (EISA) that gave NIST a leading role in the coordination and acceleration of smart grid interoperability and security standards in

collaboration with the private sector. The NIST Smart Grid program is led by the Engineering Laboratory (EL) with support from the Physical Measurement and Information Technology Laboratories. The objective of the program is to advance the measurement science that will increase asset utilization and efficiency, improve grid reliability, and enable greater use of renewable energy sources in the grid through research, standardization, testing and implementation of the NIST Smart Grid Interoperability Framework.

In the Spring of 2017, the Smart Grid Interoperability Panel (SGIP) merged with the Smart Electric Power Alliance (SEPA). SEPA's Smart Grid Cybersecurity Committee (SGCC) is led by an ITL representative. The SGCC conducts regular outreach regarding cybersecurity issues related to the smart grid, including such topics as identity and key management. Examples of this outreach include bi-weekly calls and support to the SEPA Grid Evolution Summit held on July 25-27, 2017 in Washington, D.C., where the SGCC held its annual face-to-face meeting and included a presentation on the public key infrastructure by ACD's Tim Polk. In addition to participating in SEPA's SGCC, CSD and ACD personnel are participating in SEPA's OpenFMB working groups to support cybersecurity capabilities.

In FY 2017, researchers from ITL worked on defining a grid edge experiment to understand the performance impact of cybersecurity capabilities on resource-constrained components of the grid. In addition, researchers explored how to leverage and incorporate cybersecurity risk management into the next version of the Smart Grid Interoperability Framework. ITL experts supported the Department of Energy (DoE) Cyber Resilient Energy Delivery Consortium (CREDC) program by participating in their Annual Industry Workshop in Tempe, AZ and program peer review held in Washington, D.C. Through a grant to the University of New Hampshire, NIST supported research into adding security mechanisms to the IEEE 1588 *Precision Time Protocol (PTP)*.

In FY 2018, ITL will continue to coordinate with EL and the Smart Grid Program in the development of the next version of the NIST Smart Grid Interoperability Framework 2.0 and in an execution of the grid edge experiment on the NIST Smart Grid Testbed. ITL will continue to chair SEPA's SGCC and support the DoE CREDC program, and will look for and explore opportunities to collaborate with the National Renewable Energy Laboratory (NREL) about smart grid cybersecurity.

FOR MORE INFORMATION, SEE:

https://www.nist.gov/engineering-laboratory/smart-grid
https://www.nist.gov/programs-projects/cybersecurity-smart-grid-systems
https://sepapower.org

CONTACT:

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

SOFTWARE ASSURANCE & QUALITY

Outstanding computer security is based on software implementations that minimize the existence of vulnerabilities. To develop processes that deliver high-quality software, it is vital to be able to find, characterize, and categorize vulnerabilities, weaknesses, and faults that appear in code. Processes can then be improved to preclude these faults, detect them earlier, or build in mitigations for them. The NIST Software Assurance Metrics And Tool Evaluation (SAMATE) program promotes effective software assurance processes and also evaluates methods for automated tools to provide confidence that software is free from vulnerabilities. The SAMATE program has three primary components: the Software Assurance Reference Dataset (SARD), the Static Analysis Tool Exposition (SATE), and the Bugs Framework (BF).

SARD is a public repository of hundreds of thousands of computer programs with known security flaws (see https://samate.nist.gov/SARD). The programs are primarily in five computer languages, C, C++, Java, PHP, and C#, and include synthetic test cases (small programs written as tests), open-source production programs, and production programs with vulnerabilities injected. See Figure 9 for a graph of the size, type, and languages of the test cases. This rich collection allows software developers to assess tools

and helps tool developers to refine their techniques. SARD includes contributions from government organizations, such as the Defense Advanced Research Project Agency (DARPA), the National Security Agency (NSA), the Intelligence Advanced Research Projects Activity (IARPA), academia, and industry. In FY 2017, mobile applications and test cases used in former Static Analysis Tool Expositions were added to SARD.

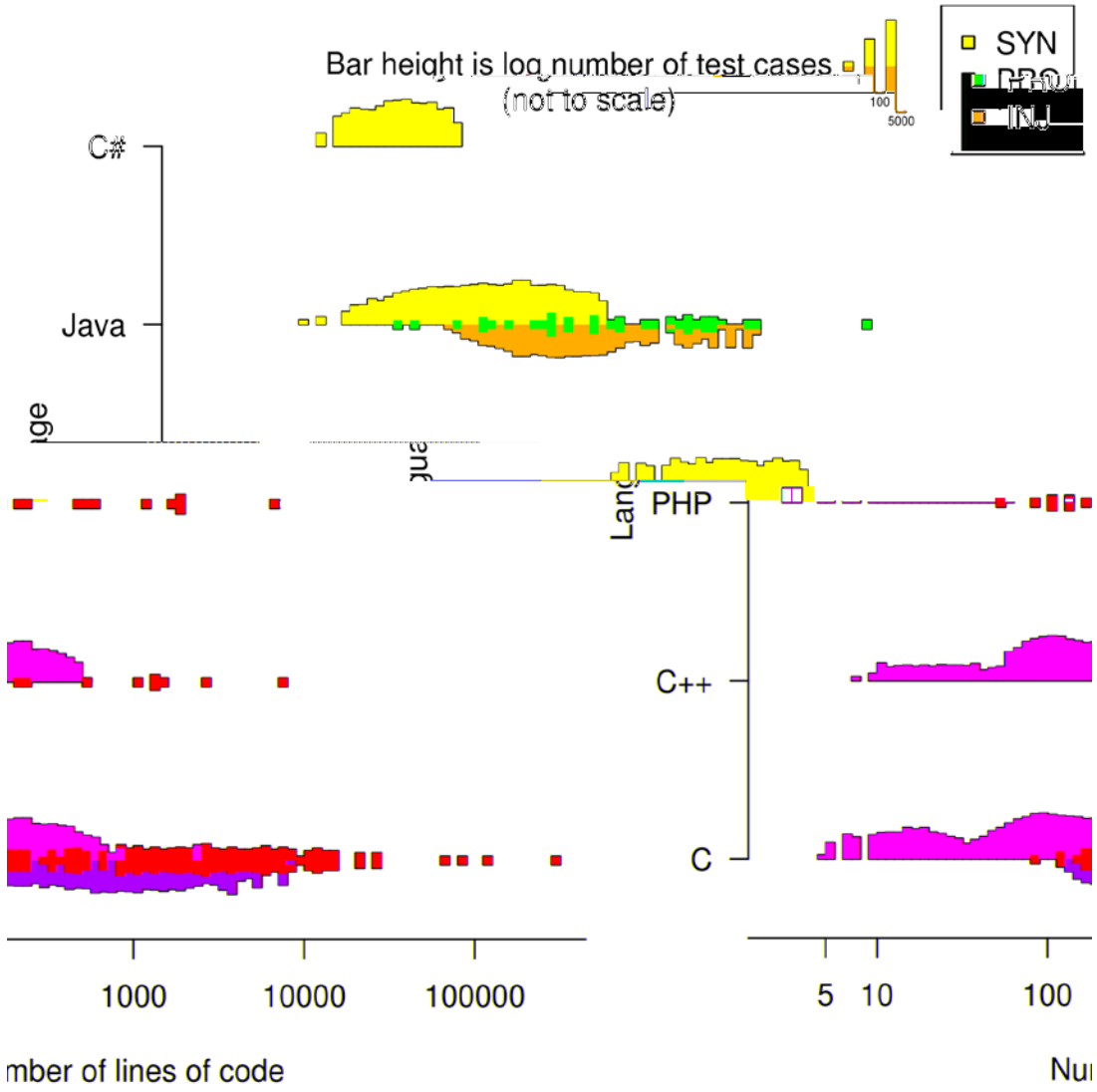


Figure 9: Graph of Size, Type, and Languages Of Test Cases in SARD

The sixth instance of SATE began in FY 2017. The SAMATE prepares test cases to measure the strengths of tools in finding source code that may lead to serious breaches. More than a dozen tool makers will run their software analysis tools on these test cases. NIST researchers, aided by others in the software assurance community, analyzed the tool reports and publicly reported their experiences at a workshop. The purpose of SATE is to understand the state of technology and society's justified confidence in software. SATE VI has three tracks: the classic track, a track to assess mobile application vetting services, and the Ockham track for sound analysis. For more information, see https://samate.nist.gov/SATE.html.

Just as the medical profession has vocabulary to precisely indicate anatomy, symptoms, and diseases, the BF seeks to improve the science of secure software by providing orthogonal, unambiguous language for software professionals. The BF comprises classes of software faults, including their attributes, causes, and consequences. Figure 10 illustrates the causal graph for buffer overflow (BOF) faults. FY 2017 updates include eight classes (including three cryptography classes):

1. Injection (INJ)–SQL, OS, etc.;
2. Control of Interaction Frequency (CIF);
3. Buffer Overflow (BOF);
4. Faulty Operation (FOP)–integer overflow, divide by zero, etc.;
5. Memory Allocation (MAL)–double free, use after free, etc.;
6. Encryption (ENC)–including decryption,
7. Verification (VRF), and
8. Key Management (KMN).

Definitions, examples, and causal graphs of these classes and links to publications are available at https://samate.nist.gov/BF.

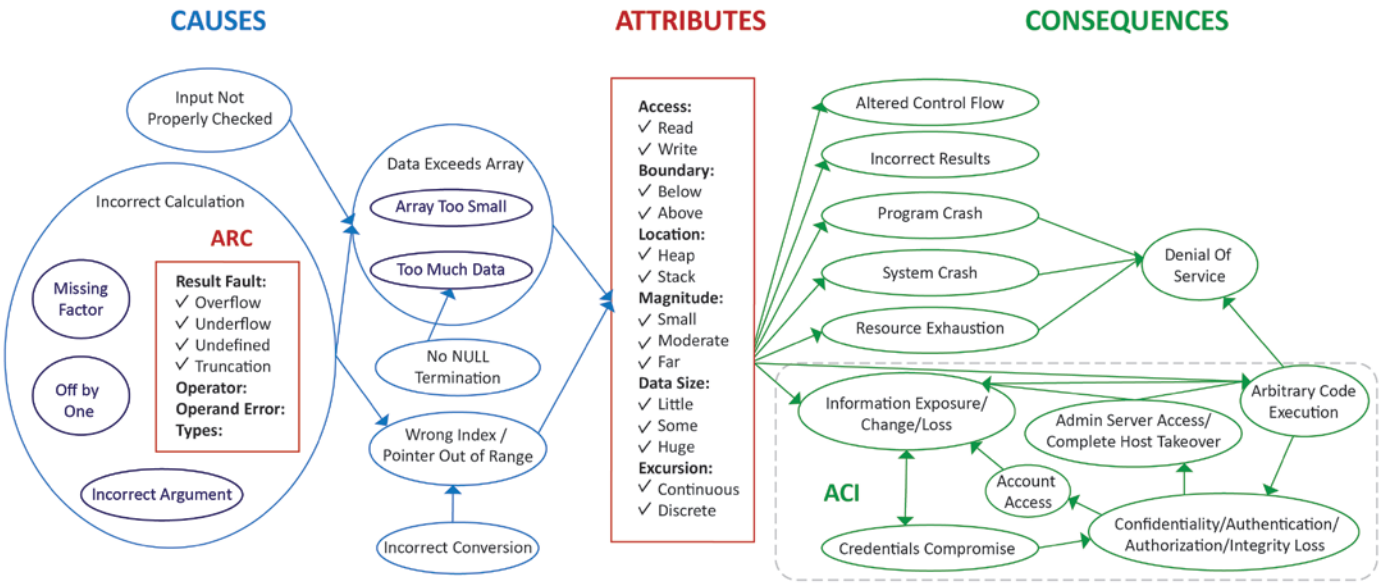


Figure 10: Causal Graph for Buffer Overflow

CONTACT:

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

FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT (R&D)

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 remained committed to the value of communicating its R&D efforts to other federal colleagues and identifying the opportunities to support R&D efforts throughout the Federal Government.

NIST is a consistent presence at the monthly cybersecurity meetings with Bill Newhouse, National Cybersecurity Center of Excellence (NCCoE) Security Engineer and the National Initiative for Cybersecurity Education (NICE) Deputy Director, as the co-chair of the Cyber Security and Information Assurance Interagency Working Group (CSIA IWG). During FY 2017, NIST provided updates to the CSIA IWG describing the updates to the NIST Cybersecurity Framework, SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, and the NICE program.

Naomi Lefkowitz, Senior Privacy Policy Advisor at NIST, co-chairs the Privacy R&D IWG, which coordinates the multidisciplinary research and development conducted by NITRD agencies that seek to produce knowledge and technologies that identify and mitigate emerging risks to our privacy, and that enables individuals, companies, and the government to benefit from technological advancements while being able to effectively balance the resulting benefits with resulting risks to privacy. The activity involves research into and development of methods for characterizing privacy expectations, understanding privacy violations, engineering privacy-protecting systems, recovering from privacy violations, and the impact of privacy on public policy and of public policy on privacy.

Ram Sriram is the co-chair of NITRD's Software Productivity, Sustainability, and Quality (SPSQ) Interagency Working Group (IWG). Robert B. Bohn is the co-chair of NITRD's Faster Administration of S&T Education and Research (FASTER) Community of Practice (CoP). Barry I. Schneider is co-chair of High End Computing (HEC) IWG. Chris Greer and Al Wavering from NIST's Engineering Laboratory co-chair NITRD's Cyber Physical Systems (CPS) IWG and the High Confidence Software and Systems (HCSS) IWG, respectively.

Tim Polk is the principal NIST participant in the bi-weekly 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 and Technology Council's Committee on Homeland and National Security.

All the NIST leaders for interagency coordination leverage these working groups and committees to communicate powerfully about NIST's research, frameworks, and publications and bring back insights and activities relevant to NIST's work.

FOR MORE INFORMATION, SEE:

https://www.nitrd.gov

CONTACT:

Mr. Bill Newhouse
(301) 975-0232
william.newhouse@nist.gov

COMPUTER FORENSICS

Digital evidence includes software, hardware, and data on computers and mobile devices (e.g., audio, video, and image files). 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 (NSRL) – a

vast archive of published software applications that is an important resource for both criminal investigators and historians.

National Software Reference Library

The 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.

The RDS continues to be the premier software resource and, in FY 2017, the NSRL published four releases. There are currently 23,000 microcomputer applications and 160,000 mobile device applications yielding a combined total of 326 million files. In FY 2017, the NSRL was expanded to include mobile applications and to include the profiles obtained from installing and exercising applications.

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. The project team's approach for testing computer forensic tools is based on well-recognized international methodologies for conformance testing and quality testing that ensures that forensic software tools consistently produce accurate and objective test results.

In FY 2016, the CFTT project expanded to allow forensics testers to use the NIST testing methodology in their own labs and to produce standardized test reports for disk imaging forensic tools. In FY 2017, federated testing was further expanded with three major updates: a revision to disk-imaging testing, the addition of mobile device tool testing and hardware write-blocker testing. In FY 2018, the project will be expanded to support string searching and forensic media preparation. The forensic community is beginning to use federated testing to test tools and share test reports. The CFTT project also maintains the Forensics Tool Catalog and the Computer Forensics Reference Data Sets (CFReDS). The Tool Catalog website is a community-sourced catalog of forensic tools aided by a taxonomy of forensic tools. The Tool Catalog grew by 17 tools in FY 2017. The CFReDS data sets are used in a variety of settings, such as university classes, to try out forensics tools on known data.

FOR MORE INFORMATION, SEE:

https://www.nsrl.nist.gov,
https://toolcatalog.nist.gov,
https://www.cfreds.nist.gov, and
https://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

Figure 11: The Seven Categories of the NICE Framework

CYBERSECURITY AWARENESS, TRAINING, EDUCATION, AND OUTREACH

National Initiative for Cybersecurity Education (NICE)

Since 2010 NIST's National Initiative for Cybersecurity Education (NICE) seeks to foster, energize, and promote a robust network and an integrated ecosystem of cybersecurity education, training, and workforce development. NICE has been focusing on efforts to achieve this by aligning to three goals: 1) accelerate learning and skills development, 2) nurture a diverse learning community, and 3) guide career development and workforce planning.

In support of goal 1, in November 2016, CyberSeek was launched to provide a visualization of the demand for and supply of cybersecurity workers across the nation (see http://cyberseek.org). At its launch, the tool also provided a visualization of career pathways in cybersecurity. The data from this tool, in part, has helped NICE develop an executive overview white paper on Cybersecurity Workforce Demand. In FY 2017, NICE also supported goal one through the development of a paper regarding Cybersecurity Apprenticeships. This report and other white papers developed by NICE authors are available at https://www.nist.gov/itl/applied-cybersecurity/nice/resources/one-pagers.

In support of goal 2, NICE hosted a Veterans in Cybersecurity Workshop in March 2017. This workshop convened approximately 40 representatives of federal and state government, branches of the military, industry, and workforce development organizations to explore issues, discuss initiatives and better understand the gaps that exist in helping our veterans transition to careers in cybersecurity.

In support of goal 3, NICE published SP 800-181, *The NICE Framework*, in August 2017 (see https://nist.gov/nice/framework). The NICE Framework establishes a taxonomy and common lexicon that is to be used to describe all cybersecurity work and workers, irrespective of where or for whom the work is performed. Figure 11 shows the seven categories of the NICE Framework. These categories further break down into Specialty Areas, Work Roles, Tasks, and Knowledge, Skills, and Abilities (KSAs).

Figure 12: Clarence Williams, Lead for Government Engagement at NICE, and Rodney Petersen, Director of NICE, speak with an attendee at the CyberSecureGov Conference in Washington, D.C.

NICE continued its coordination with academic, industry and government partners throughout the year at various meetings, workshops and events. In August 2017, NICE held a workshop in Chicago, Illinois. This workshop, along with a Request for Information that NICE issued, provided information to inform work and to prepare a report to the President on the findings and recommendations about supporting the growth and sustainment of the nation's cybersecurity workforce in the public and private sectors.

In FY 2018, NICE will continue to promote and coordinate annual NICE activities such as the NICE Quarterly eNewsletter; the NICE Webinar Series; the NICE Conference to be held on November 7-8, 2017 in Dayton, Ohio; and the NICE K-12 Cybersecurity Education Conference to be held December 4-5, 2017 in Nashville, Tennessee. NICE will also kick off the first annual National Cybersecurity Career Awareness Week on November 13-18, 2017 to focus local, regional, and national interest to inspire, educate, and engage children through adults to pursue careers in cybersecurity.

FOR MORE INFORMATION, SEE:

https://www.nist.gov/itl/applied-cybersecurity/nice

CONTACTS:

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

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

Computer Security Resource Center (CSRC)

For more than 20 years, the CSRC website has provided stakeholders with significant information about ITL's cybersecurity research and testing programs. Consistently one of the most-visited websites at NIST, CSRC is used by several ITL divisions to communicate information about NIST's cybersecurity and privacy programs and projects, research, validation testing, software tools, and other areas of interest to NIST's customers in government, industry, academia and elsewhere, both within the U.S. and globally.

The CSRC website serves as a primary NIST repository of cybersecurity and privacy standards, guidelines, and technical documents. Refer to the *Publications Released in FY 2017* section of this annual report for details about the ITL Cybersecurity Program's publications released in FY 2017.

CSRC's most significant event occurred in September 2017, with the launch of a completely redesigned, content management system-based website. In addition to aligning with the main NIST website's look and feel, the new CSRC website is organized around several primary content types to make information easier to find and maintain: projects, publications, news, events and presentations. A new taxonomy of topics is used to tag content site-wide, and an online, searchable glossary of information security terminology expands on the terms identified in NISTIR 7298 Revision 2. One of the most noticeable changes is a vastly improved publications section, in terms of content, searchability, and browsing. At the end of FY 2017, the site provided detailed information about more than 1,200 of NIST's current and historical information security publications.

The CSRC Redesign Team designed the site's architecture and interface to significantly improve site navigation, search, and the ability of ITL staff to maintain and contribute content. The site also uses responsive design to greatly improve CSRC's usability on mobile devices. More than 21,000 individual content items were transferred from the legacy site, and in February 2017, ITL successfully launched a beta version of the new site. Feedback from beta-site users over seven months was incorporated by the CSRC Redesign Team to fix bugs, implement enhancements, and refine the site's look and feel. The team considered all comments it received, and made every effort to implement those suggestions. After making significant, gradual improvements to the beta site, NIST launched the new CSRC on September 18, 2017, while simultaneously retiring the legacy site.

In FY 2018, the CSRC Redesign Team will continue to enhance the content, functionality and usability of the new site, striving to provide a better and more useful experience to site users.

The CSRC team maintains an email subscription list with more than 78,000 subscribers worldwide. Subscribers receive notifications when news updates, event details, and publication information—including the release of draft publications for public comment—are posted to CSRC. To review the available lists and subscribe, visit https://csrc.nist.gov/ and in the page footer click either the envelope icon or the "Subscribe to CSRC Updates" link. Additional NIST/ITL Cybersecurity topics are available including: Federal Information Security Management Act (FISMA) news; Cybersecurity Framework; National Initiative for Cybersecurity Education (NICE); ITL's Trusted Identity Group (TIG), and several lists for the NCCoE.

FOR MORE INFORMATION, SEE:

https://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' Forum (the Forum) is sponsored by NIST to promote the sharing of security-related information among federal agencies. The Forum, which serves more than 1,000 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 to reduce possible duplication of efforts. 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. The Forum also assists NIST in establishing and maintaining relationships with other individuals and organizations that are actively addressing information security issues within the Federal Government. During FY 2017, CSD's Victoria Pillitteri and Jody Jacobs served as Co-Chairs, and Peggy Himes from ACD served as the Secretariat of the Forum, providing administrative and logistical support. Additionally, during FY 2017, the FCSM webpage was significantly restructured and updated to ensure that presentation information, both current and archived, is delivered as efficiently and effectively as possible.

The Forum maintains an extensive email subscription service/listserv. Participation in the service is restricted to those Federal and State Government employees and their designated support contractors with a role in the management of their organization's information system security program. The email listserv offers an open forum for information sharing of best practices and recommendations, and serves as a resource for this community of interest.

The Forum conducts quarterly meetings and an annual two-day conference for a discussion of current issues and topics of interest to those responsible for supporting the information security programs of federal agencies.

Discussion topics at the quarterly FCSM meetings in FY 2017 included briefings on:

- The National Cybersecurity Center of Excellence (NCCoE) - Federally Funded Research and Development Center (FFRDC),
- Developing an information security continuous monitoring (ISCM) Assessment Methodology,
- Security Automation and Continuous Monitoring,
- Demonstration of a Continuous Diagnostic Monitoring Instance,
- Guidance for Assigning New Cybersecurity Codes to Positions with IT/Cybersecurity/ Cyber-related Functions and the New Cybercareers.gov Site,
- Using Risk Management to Improve Privacy in Federal Systems,
- National Cybersecurity and Communications Integration Center (NCCIC) 101, and
- Creating a Cybersecurity Scorecard for a Federal Agency.

FY 2017's annual two-day meeting was held at NIST on June 20-21, 2017 with over 220 attendees. Presentations included the current technical, operational and management information systems security topics and updates on the information system security activities of OMB, General Services Administration (GSA), Department of Homeland Security (DHS), Department of Health and Human Services (HHS), NARA, Internal Revenue Service (IRS), National Weather Service (NOAA), Office of Personnel Management (OPM), and NIST. A first ever "ask the experts" panel was held where attendees could ask subject matter experts on security, privacy, and procurement-related questions. Most presentations from the two-day offsite and monthly meetings are available online (see https://csrc.nist.gov/Projects/Forum/Archived-Events-and-Presentations).

The following is a list of presentations that were given at the annual two-day meeting:

- Overview of SP 800-184, *Guide for Cybersecurity Event Recovery*
- FedRAMP Tailored
- Overview of the Software Quality Assurance Project and Software Assurance Marketplace
- Applying the Cybersecurity Framework in Federal Agencies: Presentation and Panel Discussion
- Top Down vs. Bottom Up Governance of Risk, What's Best?
- Cybersecurity Dashboard on a Shoestring Budget
- High Vulnerability Asset Overlay
- Pushing Computers to the Edge: Next Generation Security and Privacy Controls for Systems and IoT Devices
- Infusing Cybersecurity into the Government Acquisition Process
- Government Accountability Office Update
- "Ask the Experts" Panel
- NIST Interagency Report 8011, *Automation Support for Security Control Assessments*

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 and State security program managers.

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/Projects/Forum

CONTACTS:

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

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

Federal Information Systems Security Educators' Association (FISSEA)

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

FISSEA membership is open to information system security professionals, professional trainers and educators, and managers responsible for information system security training programs in federal agencies, as well as contractors of these agencies and faculty members of accredited educational institutions who are involved in information security training and education. Willingness to share products, information, and experiences is all that is required to become a FISSEA member. A working group meets monthly to administer business activities.

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

The 30th Annual FISSEA Conference occurred on June 19, 2017 at NIST. The FISSEA audience included managers 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. Clarence Williams, Peggy Himes, Gretchen Morris (DB Consulting Group/NASA), and other members of the FISSEA Working Group, were integral to the effort to support the conference.

This year's theme was "Securing the Future to Infinity and Beyond: Improving Cybersecurity through Awareness, Training, and Education". Attendees gained new techniques for developing/conducting training, cost-effective practices, considerations for

compliance, and free resources and contacts. Over 150 cybersecurity training professionals attended the one-day conference.

NIST's ITL Director, Charles Romine, welcomed attendees to the event. FISSEA Lifetime Member, Louis Numkin, provided a historical timeline of FISSEA, recognizing 30 years of providing a platform for security specialists to collaborate, network, and learn.

Presenters represented NIST, DHS, DoD, HHS, private industry, and academia. Attendees had an opportunity to share about their specific awareness and training programs throughout the conference.

The FISSEA Educator of the Year Award was established to recognize and honor a contemporary who is making special efforts to create, build, manage, or inspire an information systems security awareness, training, or education program. Gretchen Morris, 2015 FISSEA Educator of the Year, presented the 2016 FISSEA Educator of the Year Award to Professor Sushil Jajodia of George Mason University. Mrs. Morris shared Mr. Jajodia's contributions to the cybersecurity education industry by characterizing his contributions in three ways: as an educationist, a researcher, and a thought leader. Professor Jajodia was presented with a plaque as recognition of his achievements in the security community.

Other traditional FISSEA conference events included announcing the winners of the FISSEA security contest. The FISSEA Security Awareness, Training & Education Contest includes five categories from one of FISSEA's three key areas of Awareness, Training, and Education. A winner is selected from each category and awarded a certificate. The categories include: (1) an awareness poster; (2) an awareness website; (3) a motivational item (e.g., trinkets, pens, stress relief items and t-shirts); (4) an awareness newsletter; (5) an interactive scenario/exercise; and (6) an awareness video

2017 FISSEA Awareness, Training, and Education Contest Winners

Awarded Certificates at the Conference (selected by an impartial judging committee prior to the conference):

- **Poster**: *K Rudolph, G. Mark Hardy, Niomi Rosenberg, Andrew Ellis, John Ippolito, & Sam Carter,* Native Intelligence, Inc. and Friends
- **Website**: *The Security Training and Awareness Program Team*, Employment and Social Development Canada (ESDC).
- **Motivational Item**: *K Rudolph*, Native Intelligence, Inc.
- **Newsletter**: *IHS Policy & Security Awareness Team,* Indian Health Service
- **Security Training Scenarios**: *Division of Information Security; Policy & Security Awareness Team*, Office of Information Technology, Indian Health Service
- **Video**: *Rita John, John Creery, Chelsea O'Hara, Nellie MacNeil, Kyle Bachan, Tim Herman, Rosanne Trudel, & Sapna Kalhan,* IFDS Canada

Publicly available YouTube video Uniform Resource Locator (URL): https://youtu.be/KBJCO6F4r2g

Peer's Choice Awards (selected by peers during the conference):

- **Poster**: *K Rudolph, G. Mark Hardy, Niomi Rosenberg, Andrew Ellis, John Ippolito, & Sam Carter,* Native Intelligence, Inc. and Friends
- **Website**: *Valerie Hayward*, InfoSight, Inc.
- **Motivational Item**: *K Rudolph*, Native Intelligence, Inc.
- **Newsletter**: *Kim Brumley, Margaret McDermott, Hiyan Sisson & Robert Cunningham,* Department of Veterans Affairs
- **Security Training Scenarios**: *K Rudolph, Niomi Rosenberg & Sam Carter,* Native Intelligence, Inc. and Friends
- **Video**: **TIE** *Rita John, John Creery, Chelsea O'Hara, Nellie MacNeil, Kyle Bachan, Tim Herman, Rosanne Trudel, & Sapna Kalhan,* IFDS Canada and *Cheryl Seaman* & *Stephanie Erickson*, The National Institutes of Health

FISSEA attendees have reported that social interaction and networking at the conference are beneficial. The conference continues to be a valuable forum for individuals from government, industry, and academia who are involved with developing, maintaining, and/or supporting security programs. Attendees gain insights regarding information security awareness, training, education, certification, and professionalization. Attendees also learn of ongoing and planned training and education programs and cybersecurity initiatives. The conference provides NIST with the opportunity to provide assistance to departments and agencies as they work to meet their FISMA responsibilities. The FISSEA website provides links to the conference program and presentations (see https://csrc.nist.gov/Projects/Federal-Info Systems-Security-Educators-Assoc.)

The next conference will be held at NIST on March 14-15, 2018.

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. Rae'chell Finch
(202) 482-0935
raechell.finch@nist.gov

Information Security and Privacy Advisory Board (ISPAB)

Since the inception of this Advisory Board in 1987, the Information Security and Privacy Advisory Board (ISPAB) has successfully renewed its charter with proper authority every two years. 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. Title III of the E-Government Act of 2002 reaffirmed the need for this Board by giving it an additional responsibility: to thoroughly review all of the proposed information technology standards and guidelines developed under Section 20 of the National Institute of Standards and Technology Act (15 U.S. Code (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 Board was originally created by the Computer Security Act of 1987 (P.L. 100-235) as the Computer System Security and Privacy Advisory Board (CSSPAB) within the Department of Commerce. The CSSPAB was chartered in May 1988 in accordance with the Federal Advisory Committee Act, as amended. The 2002 FISMA legislation amended the statutory authority of the Board and provided its current name.

The duties of the Board, as stipulated in FISMA, include:

- Identification of emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy;
- Advising NIST, DHS and the Director of the OMB on information security and privacy issues pertaining to Federal Government information systems (including the thorough review of proposed standards and guidelines developed under 15 U.S.C. 278g-3 - Computer Standards Program); and
- Annually reporting its findings to the Secretary of Commerce, the Director of the OMB, the Director of NSA, and the appropriate committees of Congress.

Congress indicated the long-term need for the Board by setting the term of Board members to four years. The charter requires that the NIST Director appoint the Chairperson and all 12 members of the Board. They are selected for their preeminence in the information technology industry or related disciplines.

The charter stipulates that Board members be selected from three main categories, with each category providing four members. Category 1 includes members from outside the Federal Government who are eminent in the information technology industry, at least one of whom is a representative of small or medium-sized companies in such industries. Category 2 also includes members from outside the Federal Government who are eminent in the field of information technology or related disciplines, but who are not employed by or representative of a producer of information. Category 3 includes those from the Federal Government who are experienced

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

Chris Boyer is currently the Chair of ISPAB. Mr. Boyer, the Assistant Vice President for Global Public Policy at AT&T, joined the Board in 2012 and assumed the responsibilities of the Chair in January 2016 (see list of Board members https://csrc.nist.gov/Projects/ISPAB/Members).

During FY 2017, ISPAB held three meetings, all in Washington, D.C.:

- June 28-30, 2017;
- March 29-31, 2017; and
- October 26-28, 2016.

In keeping with previous practices at the first meeting of each fiscal year, the Board established a work plan for FY 2017. The resulting plan included the following areas of focus:

- Cryptography, and specifically NIST R&D;
- Metrics – success measures for security and privacy;
- Trust in NIST (accountability and success);
- Quantum-resistant encryption;
- Identity management;
- Privacy engineering;
- FISMA – Continuous Diagnostics and Mitigation (CDM) and Federal Risk and Authorization Management Program (FedRAMP);
- High-Value Asset cybersecurity;
- Cybersecurity; and
- Updates of other critical NIST publications.

In aligning with the work-plan focus areas, the Board expanded its work to include the following:

- Acquisition, Supply Chain Security, and Open Source trustworthy software;
- Mobile Devices and the Protection of Sensitive Information;
- Machine Learning and Artificial Intelligence;
- The NIST Cybersecurity Framework;
- The Federal Information Security Management Act (FISMA);
- Emerging Technologies; and
- The National Cybersecurity Center of Excellence (NCCoE).

The presenters at each Board meeting were leaders and experts representing private industry, academia, federal agency Chief Information Officers (CIOs), Inspector Generals (IGs) and Chief Information Security Officers (CISOs).

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 work in information security and privacy may email their name, affiliation, and address to Matthew Scholl at the address below.

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/Projects/ISPAB

CONTACT:

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

Small and Medium Size Business (SMB) Cybersecurity Outreach Program

Small- and medium-sized businesses (SMBs)—representing approximately 95% of all businesses—

are the backbone of the U.S. economy. SMBs cannot always justify an extensive security program or even full-time staff devoted to information security. Faced with limited resources and budgets, SMBs need practical solutions and training that enable them to cost-effectively address their cybersecurity risks. NIST has partnered with other federal agencies and public-private organizations to help address these needs.

During FY 2017, the Small Business Outreach Program accomplished the following:

- Partnered with other federal agencies to catalog and evaluate existing cybersecurity educational materials designed for SMB use;
- Collaborated with federal partners, led by the Small Business Administration (SBA) and the Department of Homeland Security (DHS), on the development of the Small Business Development Center Cyber Strategy;
- Reviewed available SMB training programs from federal partners and the National Cyber Security Alliance (NCSA);
- Evaluated existing NIST SMB-focused educational materials such as reports, presentations, and online content;
- Updated the Small Business Corner website to reflect program updates and simplify SMB contact with NIST;
- Initiated the development of the NIST strategic plan for small business outreach, reflecting requirements in new Congressional legislation; and
- Published Revision 1 of NISTIR 7621, *Small Business Information Security: The Fundamentals*. This publication presents cybersecurity fundamentals for SMBs in straightforward, non-technical language (see https://www.nist.gov/publications/small-business-information-security-fundamentals).

In FY 2018, the Small Business Outreach Program will continue to collaborate with federal and other partners to understand the cybersecurity needs of SMBs and identify and/or develop materials and training to meet those needs.

FOR MORE INFORMATION, SEE:

https://www.nist.gov/programs-projects/small-business-corner-sbc

CONTACTS:

Email: smallbizsecurity@nist.gov

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

Ms. Marian Merritt
(240) 338-2033
marian.merritt@nist.gov

Mr. Jeff Marron
(301) 975-3846
jeffrey.marron@nist.gov

Mr. Matthew Barrett
(301) 975-3267
matthew.barrett@nist.gov

CRYPTOGRAPHIC STANDARDS PROGRAM

Cryptographic Hash Algorithms

Cryptographic hash functions, which transform arbitrarily long input data into a fixed-length output, are a fundamental tool for information security, e.g., digital signatures, pseudorandom functions, and key derivation.

NIST has standardized two families of Secure Hash Algorithms (SHA): SHA-1 and SHA-2 in Federal Information Processing Standard (FIPS) 180, and SHA-3 in FIPS 202.

The SHA-1 function—which was published in the original version of FIPS 180 in 1995, and which is still specified along with the SHA-2 family in FIPS 180-4—has been deprecated for many years, because it could no longer be relied upon to provide the important property of "collision resistance." In fact, in 2017 a SHA-1 collision (different inputs with the same output) was published by researchers at Centrum Wiskunde & Informatica (CWI) Institute of Amsterdam and Google, based on the seminal cryptanalysis in 2005 by Xiaoyun Wang of Shandong University.

Wang's research was the main impetus to the development of SHA-3 through a public competition, which NIST initiated in 2007. The winning algorithm, KECCAK, was chosen in part because its components

could easily be adapted to provide a variety of functionalities.

FIPS 202 realized some of this potential by including two eXtendable Output Functions (XOFs), which allow variable-length outputs, in addition to its four hash functions. The two XOFs are called SHAKE128 and SHAKE256; the numerical suffix indicates the supported security strength. FIPS 202 also supports a flexible scheme for "domain separation" between different functions, which ensures that different named functions will produce unrelated outputs.

In December 2016, NIST further expanded the uses of KECCAK with the publication SP 800-185, *SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash*. It provides four new types of functions, as indicated in the title, each with the same two supported security strengths:

- cSHAKE128 and cSHAKE256 are XOFs that can be "customized" for individual users or applications, so that their outputs would be unrelated to any other SHAKE variants;
- KMAC128 and KMAC256 are keyed-hash functions with variable-length outputs, i.e., pseudorandom functions (PRFs);
- TupleHash128 and TupleHash256 are hash functions on tuples of input strings; and
- ParallelHash128 and ParallelHash256 are hash functions that can exploit parallel processing to efficiently hash long messages.

NIST is currently considering the development of a parallelizable hashing mode and XOF mode for generic hash functions (e.g., SHA-2). These modes would allow the SHA-2 family to achieve some of the functionality of the SHA-3 family.

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/projects/hash-functions/sha-3-standardization

CONTACT:

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

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

Triple Data Encryption Algorithm (TDEA)

SP 800-67: *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher:*

The TDEA algorithm is specified in SP 800-67 Revision 1. This publication includes a specification of the Data Encryption Algorithm (DEA) engine that was originally specified in FIPS 46, *The Data Encryption Standard*, in 1977 and was withdrawn as an approved algorithm in 2005.

A security analysis and practical demonstration of attacks on TDEA in several real-world protocols was posted in FY 2017 by Karthikeyan Bhargavan and Gaëtan Leurent of Inria (Paris) and is available at https://sweet32.info/. This article provides evidence that the collision attack on TDEA represents a serious security vulnerability for many common uses of these protocols — including the Hyper Text Transfer Protocol Secure (HTTPS) protocol for secure Internet connections. Moreover, the analysis shows that the security vulnerability remains serious unless more stringent limits are imposed on the amount of data that can be encrypted under a single three-key bundle than the current data limit recommended by NIST in SP 800-67, Revision 1.

In response to this article, NIST posted a notice announcing plans to reduce the maximum amount of plaintext allowed to be encrypted under a single TDEA three-key bundle from 2^{32} to 2^{20} (64-bit) blocks, and to revise SP 800-67 accordingly. In addition, NIST plans to disallow TDEA for TLS, IPsec and possibly other protocols (see https://csrc.nist.gov/News/2017/Update-to-Current-Use-and-Deprecation-of-TDEA for the announcement).

In late FY 2017, a revision of SP 800-67 was provided for public comment that included the above restriction on the usage of TDEA for each three-key TDEA key bundle. SP 800-67 Rev 2 will be published in early FY 2018.

CONTACT:

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

Random Bit Generation

Random bits are required for the secure use of most cryptographic algorithms. For example, random bits are used to generate the keys needed for encryption and digital signature applications. CSD began work on the specification of random bit generators in the late 1990s. Information on the Random Bit Generation project is available at https://csrc.nist.gov/projects/random-bit-generation.

This project consists of the development of three NIST Special Publications (SPs). SP 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, was initially published in 2007 and last revised in 2015. It 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 the latest drafts were made available for public comment in 2016 via the Special Publications page: https://csrc.nist.gov/publications/PubsSPs.html.

SP 800-90B, *Recommendation for the Entropy Sources Used for Random Bit Generation*, addresses the development and testing of entropy sources. Figure 13 illustrates the model that the Recommendation uses to describe an entropy source and its components: a noise source, health tests, and an optional conditioning component.

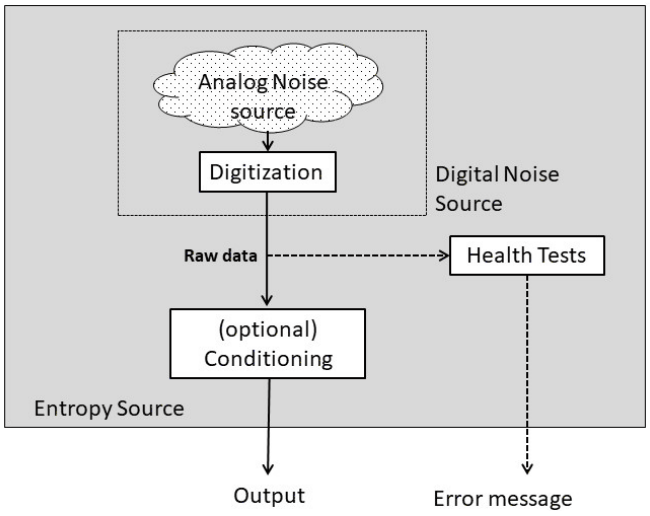


Figure 13: Entropy Source Model

In Figure 13, the noise source contains the entropy-providing activity (e.g., the output of 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) and Cryptographic Module Validation Program (CMVP) to validate candidate entropy sources. During FY 2017, CSD finalized the test descriptions for the initial publication of SP 800-90B, which is expected to be published in early FY 2018. CSD will begin a revision of the document in FY 2018 to address issues that were not included in the initial version of the document and any lessons learned during validation testing by the CAVP and CMVP labs.

The initial version of SP 800-90B will be available via the Special Publications page: https://csrc.nist.gov/publications/PubsSPs.html.

In May 2017, a presentation "A Tale of Two Entropy Source Validation Approaches: NIST 800 90B vs. BSI AIS 31" was provided by Meltem Sönmez Turan at the ICMC17 International Cryptographic Module Conference held in Washington D.C.

SP 800-90C, *Recommendation for Random Bit Generator (RBG) Constructions*, 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 (DRBGs; also known as pseudorandom number generators). Two general models are provided in SP 800-90C, as shown in Figure 14 and Figure 15.

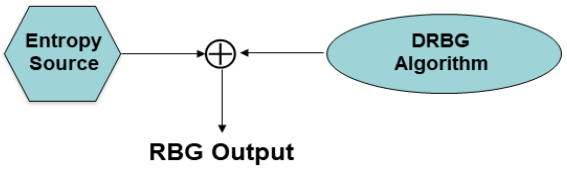


Figure 14: XOR-NRBG

Figure 14 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 15: DRBG and Oversampling NRBG

Figure 15 depicts the construction used for the DRBGs and the second NRBG design – the Oversampling NRBG. In this construction. the entropy source repeatedly provides input to the DRBG algorithm to produce the requested output.

The difference between DRBGs and NRBGs 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: https://csrc.nist.gov/publications/PubsSPs.html.

Plans for FY 2018:

The RBG development team has the following goals for FY 2018:

- Publish the initial version of SP 800-90B and post the comments received during the last public comment period, along with their resolutions. The testing of entropy sources by the CAVP and CMVP will begin as soon as possible after publication.
- Monitor the testing of SP 800-90B in the CAVP and CMVP labs to determine problems that need to be addressed in the next version of SP 800-90B. In some cases, the problems may be addressed by additions to the FIPS 140-2 Implementation Guidance document until SP 800-90B is revised. The Implementation Guidance document is available at https://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf.
- Begin a revision of SP 800-90B to address issues not included in the initial version of SP 800-90B, as well as any issues that surface during CAVP and CMVP entropy source validation.
- Finalize and publish 800-90C, posting the comments received and their resolution, along with the document.
- Complete plans for testing SP 800-90C.

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/projects/random-bit-generation

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

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) (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 helping other institutions set up 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. It is expected that the University of Chile will start operating their own randomness beacon during FY 2018.

As of the end of FY 2017, the NIST Beacon has been functioning without major interruptions for more than four years. During this time, the project team has received valuable input from a growing community of users. As a result, the project team has redesigned the Application Programming Interface (API) and the architecture. The changes provide higher security and availability, as well as better interoperability. Version 2.0 of the NIST Beacon is scheduled to be deployed during November 2017.

NIST encourages the community of users 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. René Peralta
(301) 975-8702
rene.peralta@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 common 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 https://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), 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 EaaS 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 16. 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 first in, first out (FIFO)-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 copied 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. Recently, an alternative innovative technology has emerged that allows extracting unique cryptographic keys from the imperfections of memory Static Random Access Memory (SRAM) cells used in common computers. The idea behind this technology is to extract PUF-like unique data from the SRAM chip, which is then used to construct a unique key. This technology is quite interesting for EaaS applications on the client side because it eliminates the need to provision an initial key for accessing EaaS. If a client system or device does not 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 the Hyper Text Transfer Protocol (HTTP) to transfer entropy payloads from the server to clients. To secure this transmission, the server encrypts the data using the client's 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.

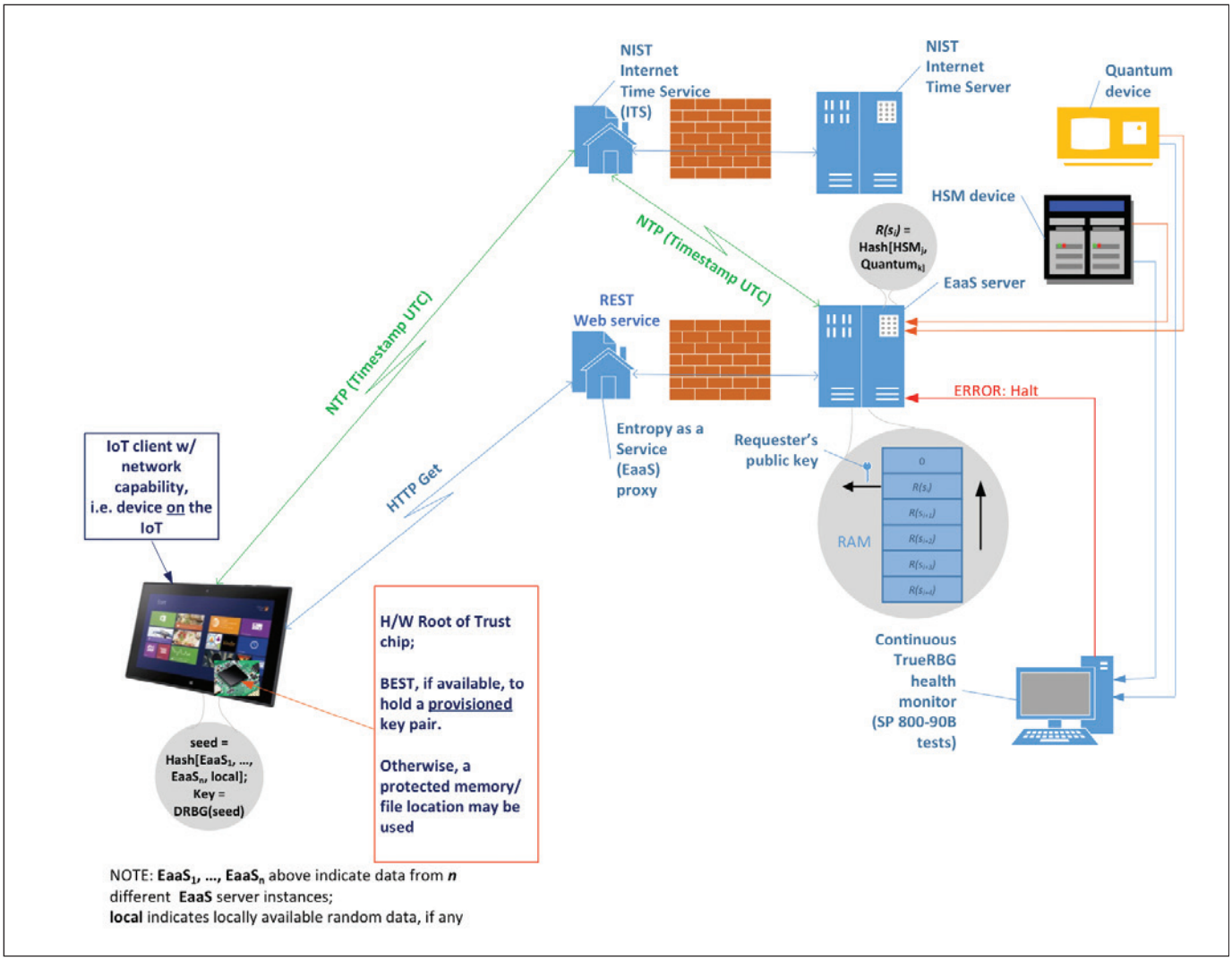


Figure 16: High-level Architecture of EaaS

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). A published paper on EaaS in IEEE Computer magazine generated a lot of interest among the public, including companies from the U.S. and Canada who approached the team and asked for assistance in implementing and hosting their own EaaS servers. The team started a technology transfer effort to help with this. The team also continues the collaboration with a team of researchers at the University of Florida who work under a NIST research grant to explore ways to leverage EaaS in protecting against integrated circuit counterfeiting and thereby help secure a supply chain. The University of Florida researchers working on this grant obtained interesting security results that identified security vulnerabilities in widely used protocols for intellectual property protection in integrated circuit manufacturing and resulted in proposals for new secure protocols that eliminated these vulnerabilities.

The team continues to develop the system to provide a publicly accessible NIST EaaS instance in FY 2018. The team succeeded in establishing a non-disclosure agreement and a collaboration with Intrinsic ID, Inc. – a company with complementing technology for constructing the initial key on the client side by extracting it from SRAM memory cells. The team also established a collaborative relationship with Crypto4A and 2Keys Corp. from Canada on

developing a common protocol for EaaS. The team coordinated with the research team working on the NIST Beacon for developing common back-end components for the two services. The team plans to leverage these common components in the NIST EaaS implementation.

CONTACT:

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

Block Cipher Modes of Operation

The engine for many of the techniques in CSD's cryptographic toolkit is a block cipher algorithm, such as the Advanced Encryption Standard (AES) algorithm. A block cipher transforms some fixed-length binary data (i.e., a "block" of data) 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 2016. It specifies two AES modes of operation, called FF1 and FF3, for "format-preserving encryption" (FPE), based on proposals that were submitted from the private sector, specifically, the payments industry.

Recently, two academic researchers, Vaudenay and Dürak, developed a cryptanalytic attack on the FF3 mode. On April 12, 2017, CSD posted an announcement that summarizes the attack and outlines CSD's plans to revise FF3 in a new draft of SP 800-38G in FY 2018; see https://csrc.nist.gov/News/2017/Recent-Cryptanalysis-of-FF3.

In FY 2018, CSD also plans to revisit SP 800-38D, which specifies the Galois/Counter Mode (GCM) for authenticated encryption. In particular, the security of GCM depends critically on the requirement for the uniqueness of the "nonce" input; CSD plans to seek public comment on how to best update the guidance for achieving this property.

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/projects/block-cipher-techniques

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 CSD began providing guidance in managing the keys used for cryptographic applications in the late 1990s to early 2000s. Information on the CSD's key management project is available at https://csrc.nist.gov/projects/key-management.

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

In FY 2017, SP 800-56A was revised. SP 800-56A was originally published in 2006, and was previously revised in 2007 and 2013. This document specifies Diffie-Hellman (DH) and Menezes-Qu-Vanstone (MQV) key-agreement schemes, both elliptic curve and finite field versions. Key agreement results in keying material that is shared between the participants. A key-agreement scheme is a procedure in which both parties contribute information that is used in generating a cryptographic key. A key-agreement scheme is defined by a cryptographic algorithm, together with 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. 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 17 below provides a simplified example of one of the key-agreement schemes. 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.

A revision of SP 800-56A was provided for public comment in FY 2017 as a draft of SP 800-56A Rev. 3. This revision includes the following changes:

- Added the KECCAK Message Authentication Code (KMAC) to the list of **approved** MAC functions; KMAC is specified in SP 800-185, *SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash*.
- The elliptic curves to be used in the elliptic curve Diffie-Hellman and MQV schemes will henceforward be specifed in SP 800-186, a new publication under development that will include the elliptic curves currently specified in FIPS 186-4, *Digital Signature Standard (DSS)*, along with additional approved elliptic curves for key agreement and digital signatures.
- The key-derivation functions were moved to SP 800-56C: Recommendation for *Key-Derivation Methods in Key-Derivation Schemes* (see below).

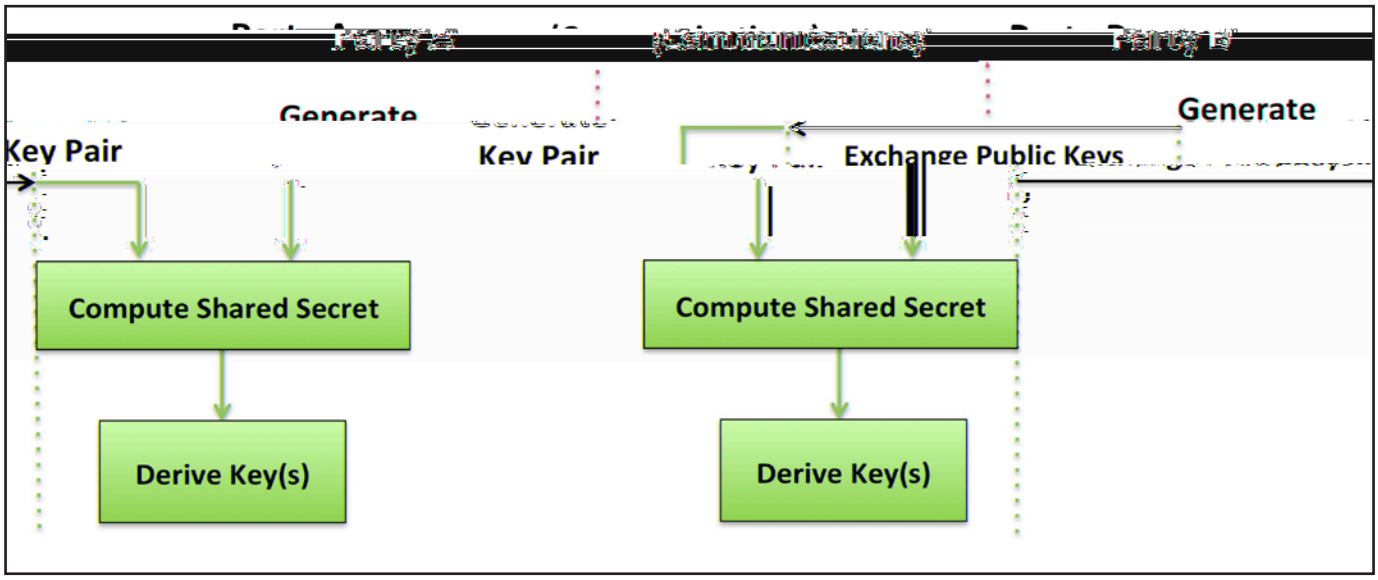


Figure 17: Key-Agreement Example

- Encourages the use of pre-defined domain parameter groups for the finite field Diffie-Hellman and MQV schemes. Domain parameters are used to generate keys and compute the shared secret. The domain-parameter groups include the "safe primes" that are used in the Transport Layer Security (TLS) and Internet Key Exchange (IKE) protocols.

A more complete list of changes is provided in an appendix of SP 800-56A Rev. 3. SP 800-56A Rev. 3 will be published in early FY 2018 and will be available via the CSD publications page at https://csrc.nist.gov/publications. This web page may also be used to access FIPS 186-4, SP 800-185, and (eventually) SP 800-186.

Information about SP 800-56A is also available at https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/draft.

SP 800-56C: *Recommendation for Key-Derivation Methods in Key-Establishment Schemes*:

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. SP 800-56A is discussed above. SP 800-56B: *Recommendation for Pairwise Key-Establishment Schemes Using Integer Factorization Cryptography*, is available via https://csrc.nist.gov/publications.

SP 800-56C had included only one method for key derivation – a two-step key-derivation procedure that used either the Keyed-Hash Message Authentication Code (HMAC) or the Cipher-based Message Authentication Code (CMAC) algorithm during the 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*. These documents are available via https://csrc.nist.gov/publications.

A revision of SP 800-56C was provided for public comment in FY 2017 as a draft of SP 800-56C Rev. 1. This revision includes the following changes:

- The single-step key derivation functions specified in SP 800-56A and SP 800-56B were moved into SP 800-56C, as well as the references to SP 800-135: *Recommendation for Existing Application-Specific Key Derivation Functions*. Note that the relevant changes to SP 800-56B (i.e., to remove the key derivation functions from the document) have not been performed yet; those changes will be initiated in FY 2018 (see below).
- KMAC, as specified in Draft SP 800-185, *SHA-3 Derived Functions*: cSHAKE, KECCAK Message Authentication Code (KMAC), *TupleHash and ParallelHash*, is allowed for the single-step key derivation functions.

Changes to the document are discussed in an appendix of SP 800-56C Rev. 1. SP 800-56A Rev. 3 will be published in early FY 2018 and will be available via the CSD publications page at https://csrc.nist.gov/publications. SP 800-135 and SP 800-185 are also available using that address.

Information on SP 800-56C is also available at https://csrc.nist.gov/publications/detail/sp/800-56c/rev-1/draft.

New Key Management Publications Under Development:

A new document was started in FY 2016 on key storage and recovery by an organization (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 2018:

During FY 2018, the CSD is expecting to accomplish the following key management tasks:

- Publish the revisions of SP 800-56A and SP 800-56C.
- Begin the revision of SP 800-56B and post it for public comment.
- Begin revisions of SP 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, to address the use of Triple Data Encryption Algorithm (TDEA), SP 800-56A, SP 800-56B, KMAC and other SHA-3 derived functions specified in SP 800-185. A statement about the advent of quantum-resistant algorithms will also be included.
- Begin revisions of SP 800-57, Part 2, *Recommendation for Key Management, Part 2: Best Practices for Key Management Organization*, to update the guidance.
- Revise SP 800-57, Part 3, *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance*, to provide revised

guidance on the use of the Internet Protocol Security (IPsec) protocol.

- Continue the development of the organizational key-storage and recovery publication.
- Resume work on SP 800-71, *Recommendation for Key Establishment Using Symmetric Block Ciphers*.

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/projects/key-management/cryptographic-key-management-systems

CONTACTS:

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

Mr. Quynh Dang
(301) 975-3610
quynh.dang@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 2014. Since the first revision, CSD has been following developments in TLS implementations, including updates and attacks. In FY 2016, a second revision was initiated that updates TLS recommendations to include mitigations for recent attacks, synchronizes cryptographic algorithm recommendations with other NIST Special Publications, and provides more flexibility to system administrators in choosing which TLS features they should support. There is also guidance for implementations of TLS version 1.3, a significant update to TLS. SP 800-52 Revision 2 will be posted for public review and comment in FY 2018.

CSD 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 2018, CSD will be contributing code to testssl.sh that adds support for TLS version 1.3. When the draft of SP 800-52 Revision 2 is posted for public comment, CSD intends to make a draft version of this code available that includes some checks for conformance to SP 800-52 Revision 2.

CONTACTS:

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

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

Cryptographic Recommendations for the Internet Protocol Security (IPsec) and Internet Key Exchange (IKE)

IPsec is a suite of protocols for securing Internet communications at the network layer and operates within the Internet Protocol (IP). It is frequently used to establish Virtual Private Networks (VPNs), requiring both parties to share keying material, which can be established using the Internet Key Exchange (IKE) protocol, and enabling telecommuters or travelers to gain secure access to their enterprise networks. IPsec provides the cryptographic security functions for both versions of the Internet Protocol, IPv4 and IPv6.

CSD has provided cryptographic guidance for using IPsec and IKE in SP 800-57 part 3, Section 3: Internet Protocol Security (IPsec). From the beginning of FY 2017, CSD has been working on a revision of the section and plans to publish it as a standalone Special Publication. This SP will update and expand the existing cryptographic guidelines. The important technical updates include disallowing Triple DES and recommending AES-GCM authenticated encryption instead of the CipherBlock Chaining (CBC) mode.

CSD expects to release the draft SP in FY 2018 for public comments. The SP will be harmonized with an upcoming revision of SP 800-77, *Guide to IPsec VPNs*.

CONTACTS:

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

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

Elliptic Curve Cryptography

Elliptic curve cryptography is critical to the adoption of strong cryptography during the migration to higher security strengths. One of the main advantages of elliptic curve cryptography is that users can achieve the same level of security as other systems, but with a much shorter key length. 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 15 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 15 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 2017, NIST utilized feedback received to revise and improve FIPS 186-4. In particular, NIST plans to add new elliptic curves to the current recommended set. The entire collection of recommended curves and their specification will be moved to a new publication SP 800-186: *Recommendations for Discrete-Logarithm Based Cryptography: Elliptic Curve Domain Parameters*. In addition, new deterministic digital signature schemes will be included in FIPS 186. It is expected that the revised draft version of FIPS 186-5 (and SP 800-186) will be available for public comment in early FY 2018.

CONTACTS:

Email project team: EllipticCurves@nist.gov

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

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

Mr. Andrew 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 (see Table 1). The focus of the Post-Quantum Cryptography (PQC) 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 2017. The presentation topics included 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.

The NIST team also continues to be productive in post-quantum cryptography research. The results have been published at major conferences, such as Real World Cryptography, Number Theory Methods in Cryptography, Selected Areas in Cryptography, Post-Quantum Cryptography (PQCrypto), and AsiaCrypt. NIST researchers have given many presentations at

TABLE 1: IMPACT OF QUANTUM COMPUTING ON COMMON CRYPTOGRAPHIC ALGORITHMS			
CRYPTOGRAPHIC ALGORITHM	**TYPE**	**PURPOSE**	**IMPACT FROM LARGE-SCALE QUANTUM COMPUTER**
AES	Symmetric key	Encryption	Larger key sizes likely needed
SHA-2, SHA-3	----------	Hash functions	Larger output likely needed
RSA	Public Key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA, DH (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

venues, such as the European Telecommunication Standardisation Institute (ETSI) Quantum-Safe Workshop, to increase awareness of the upcoming migration to post-quantum cryptography, and to engage with stakeholders in the U.S. and other countries. NIST has also sponsored other research, education, and research events.

In 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. Shortly thereafter, NIST began 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 https://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). Submitters from around the world are invited to propose quantum-resistant cryptosystems for consideration by NIST as part of the PQC standardization process. In December 2016, after resolving and assessing public comments, NIST issued the final submission requirements and evaluation criteria. NIST has received several proposals, and the final submission deadline is in November 2017.

In FY 2018, NIST will continue to explore the security and feasibility of purported quantum-resistant technologies submitted to the *Post-Quantum Standardization Process*. NIST will hold a public workshop in April 2018, co-located with the PQCrypto conference in Florida, during which submitters will be invited to present their algorithms. The *Post-Quantum Standardization Process* will proceed with multiple rounds of public evaluation and analysis, with the goal of selecting algorithms for standardization by NIST after three to five years of analysis.

FOR MORE INFORMATION, SEE:

https://www.nist.gov/pqcrypto

CONTACTS:

Email project team: pqc@nist.gov

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

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

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

Circuit Complexity

Cryptographic functions, such as those used for 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 reduce the size and depth of these circuits. Size impacts energy consumption and power requirements. Depth largely determines the speed at which the functions are evaluated by the circuit. This reduction problem is closely related to designing small (and low-depth) combinational circuits, which contain only logical gates (i.e., no registers are used, and there is no clock). Figure 18 below shows one such circuit, for performing inversion in GF(2^4).

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. CSD has developed and implemented new solutions for the circuit-minimization problem. There is a tradeoff between the size and depth of circuits. Heuristics that do well with respect to one of these metrics tend to do so at the expense of the other one. In cooperation with colleagues at the University of Southern Denmark, CSD developed a new heuristic that simultaneously reduces size and depth.

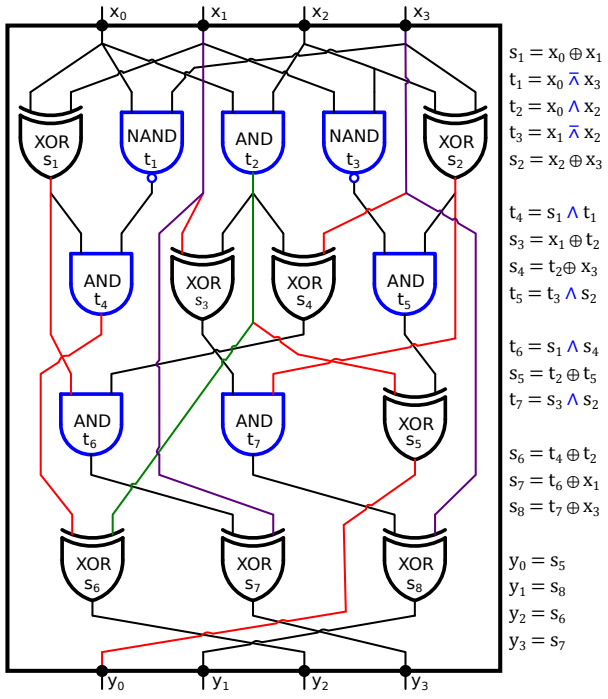


Figure 18: Inversion in GF(2^4)

CSD 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 — the number of AND gates necessary and sufficient to implement a function — is called multiplicative complexity. Unfortunately, determining multiplicative complexity is extremely hard. In previous years, the CSD was able to determine the multiplicative complexity of all Boolean functions on up to five input bits. This year the team was able to do the same for all functions on six inputs (there are 2^{64} such functions). ITL was able to exhibit specific functions on n bits which are impossible to calculate with fewer than n AND gates. Also as a result of this classification, it was possible to determine the multiplicative complexity of the symmetric function $\Sigma(8,4)$ – problems that had remained unresolved for many years.

Secure multi-party 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: 1) holding an election; 2) conducting closed-bid auctions in which only the winning bid is determined; 3) proving to a third party that a person's encrypted attributes satisfy some requirement, such as being "over 21 and (U.S. citizen or Canadian citizen)". The protocols that solve secure multi-party 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 a circuit with only a few multiplication (AND) gates is important. Some of the circuits published are now a standard reference for the benchmarking of secure multi-party computation protocols.

The results on circuit size and depth, and on multiplicative complexity were presented at the 2nd International Workshop on Boolean Functions and their Applications (Bergen, Norway). Circuits are periodically posted at https://csrc.nist.gov/Projects/Circuit-Complexity/Circuit-Problems.

CONTACT:

Dr. René 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.

In October 2016, CSD held the Second Lightweight Cryptography Workshop for representatives from government, industry, and academia. The workshop led to the publication of NISTIR 8114, *Report on Lightweight Cryptography*. This report provides an overview of the lightweight cryptography project at NIST, and describes a plan for the standardization of lightweight cryptographic algorithms. A draft whitepaper, *Profiles for the Lightweight Cryptography Standardization Process*, was released for public comment in order to receive community feedback on the goals for the first set of NIST lightweight cryptography standards. The functionality that will be requested for this first set of standards are authenticated encryption with associated data (AEAD) with optional hashing. A call for algorithm submissions for the lightweight cryptography portfolio will be announced in FY 2018, along with details of the selection process.

NISTIR 8114 and the Lightweight Cryptography project were featured in the June 2017 ITL bulletin, and CSD presented a poster on the project during ITL Science Day in October 2016. The Lightweight Cryptography project was presented at several venues in FY 2017, including Real World Crypto, HighLight: High Security Lightweight Cryptography, and the rump sessions of the Eurocrypt and Crypto conferences.

FOR MORE INFORMATION, SEE:

https://www.nist.gov/programs-projects/lightweight-cryptography
https://csrc.nist.gov/publications/detail/itl-bulletin/2017/06/toward-standardizing-lightweight-cryptography/final

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

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. CSD 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 2017, NIST researchers continuously collaborated with the IEEE 802.21 Working Group. IEEE 802.21 "Media Independent Handover Services Framework" was published, and IEEE 802.21.1 "Media Independent Services" was finalized for publication. These new standards address the future connectivity and management requirements of Smart Grid, IoT and Smart Home networks, where multimode wireless devices and smart end nodes incorporate different wireless interfaces, and need to switch among the networks during an ongoing communication session, while maintaining the same security posture. IEEE 802.21 and IEEE 802.21.1 adopted NIST standardized cryptographic algorithms, such as ECDSA, as specified in FIPS 186-4, and AES-CCM, as specified in SP 800-38C.

The recently revealed KRACK attack on the IEEE 802.11 wireless network leads to generating the same key stream in the case of AES-CCM, or recovering the authentication key, in the case of AES-GCM through a man-in-the-middle attack to create a counter reset condition. The KRACK attack confirms that it is essential to make sure that the special features and assumptions for using each cryptographic algorithm are considered in the protocol design so that the requirements are satisfied to assure security in any circumstance.

In FY 2018, CSD will continue to contribute to IEEE 802 wireless standards. CSD will work with the IEEE 802.11 working group to develop countermeasures for the KRACK attack.

CONTACT:

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

Blockchains

CSD 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 undetected modification 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 untrusted parties) agree to its accuracy. In essence, a blockchain is a mutually agreed-upon record of history.

Figure 19 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. CSD is investigating the use of blockchains to determine which application types are appropriate for using blockchains and which are not. CSD is monitoring the proposed uses of cryptography to assure that current cryptographic techniques are used properly and whether new techniques are required.

During FY 2017, NIST participated in standards activities exploring blockchain technologies, architectures, and use cases. These included participation in a new blockchain study group sponsored by American Standards Committee X9, the financial services committee of the American National Standards Institute (ANSI), and continued work in the International Standards Organization (ISO) Technical Committee (TC) for Blockchains and Distributed Ledger Technologies (ISO/TC 307). Established in 2016, the initial objectives of ISO/TC 307 include defining key terms and concepts, exploring reference architectures, investigating use cases, and identifying identity and privacy implications within blockchain technologies and architectures. NIST has

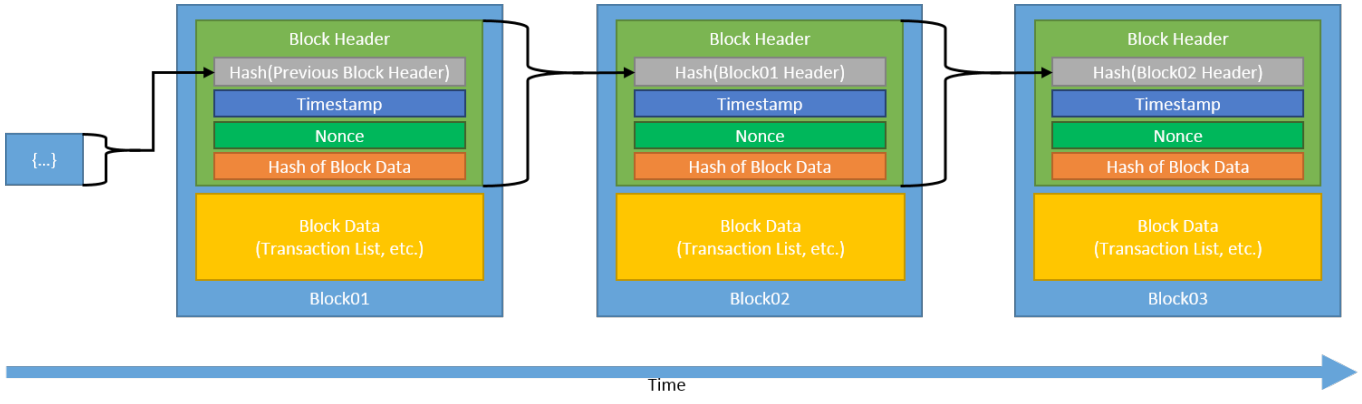


Figure 19: Example of a Blockchain

been participating in these activities via the national mirror committee within the InterNational Committee for Information Technology Standards (INCITS). ISO/TC 307 will meet in November 2017, where the reports on these topics will be reviewed and new work will be established.

During FY 2017, CSD established the *NIST Internal Blockchain Workbench* to support internal research exploring blockchain technologies and use cases. The workbench itself is hosted on internal servers, and is currently running two blockchains – the first is a permissioned blockchain utilizing the MultiChain blockchain platform; the second is Ethereum, which has been configured to run only within the workbench. In addition to the blockchain software itself, the workbench has demonstration applications with source code, software development tools and several diagnostic tool suites available for researchers to utilize. NIST/ITL plans to continue advancing the capabilities of the workbench and expanding the types of blockchains available in FY 2018.

CONTACTS:

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

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

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

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

Mr. Dylan Yaga
(301) 975-6004
dylan.yaga@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 develops test suites and test methods; provides implementation guidance and technical support to industry forums; and conducts education, training, and outreach programs.

CSD'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 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 list 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 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 https://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 FY 2017, the CAVP had issued approximately 28,710 validations, representing the algorithm validations of approximately 18 approved algorithms, including 5 modes of operation.

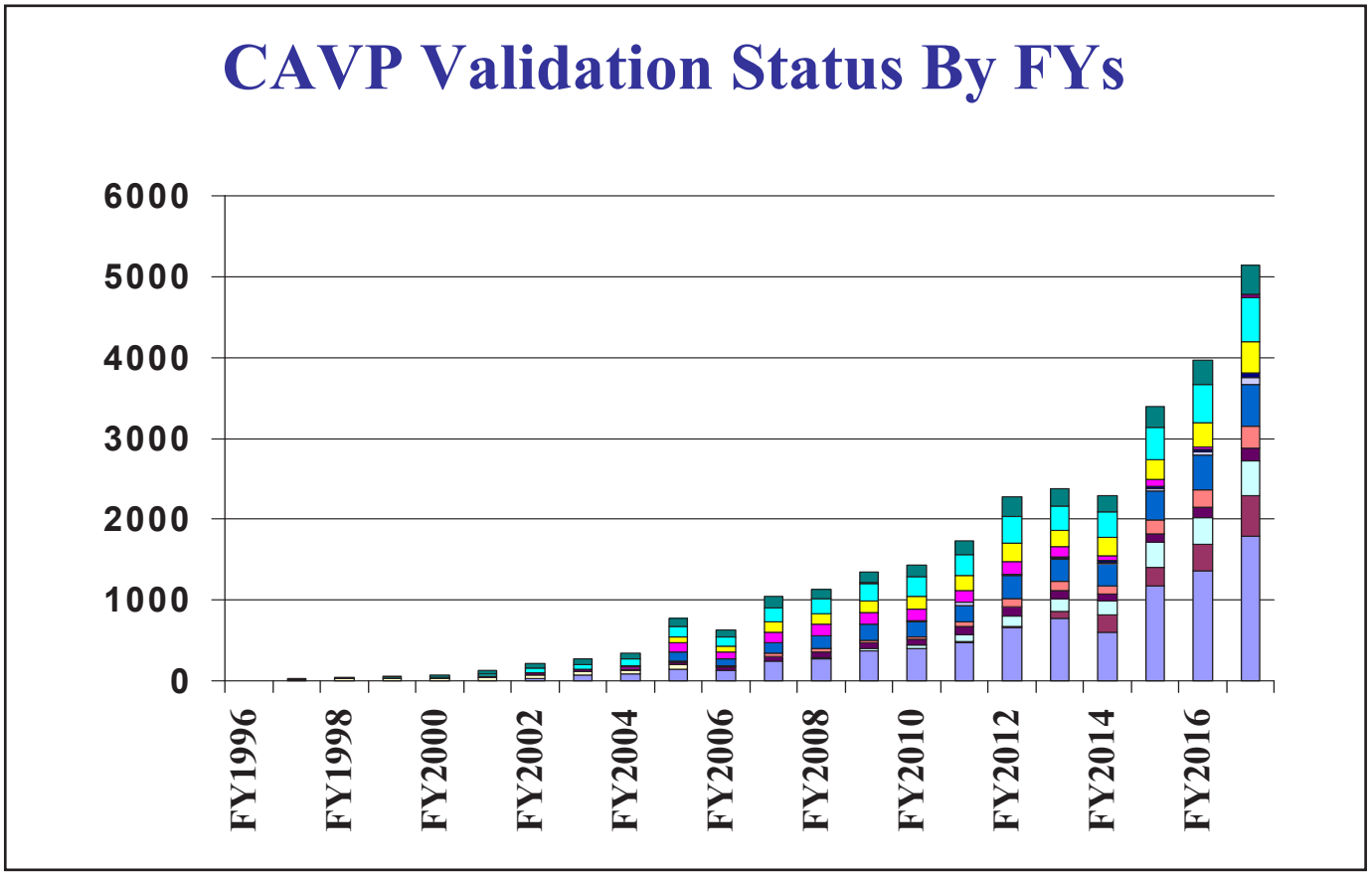


Figure 20: CAVP Validation Status by Fiscal Year

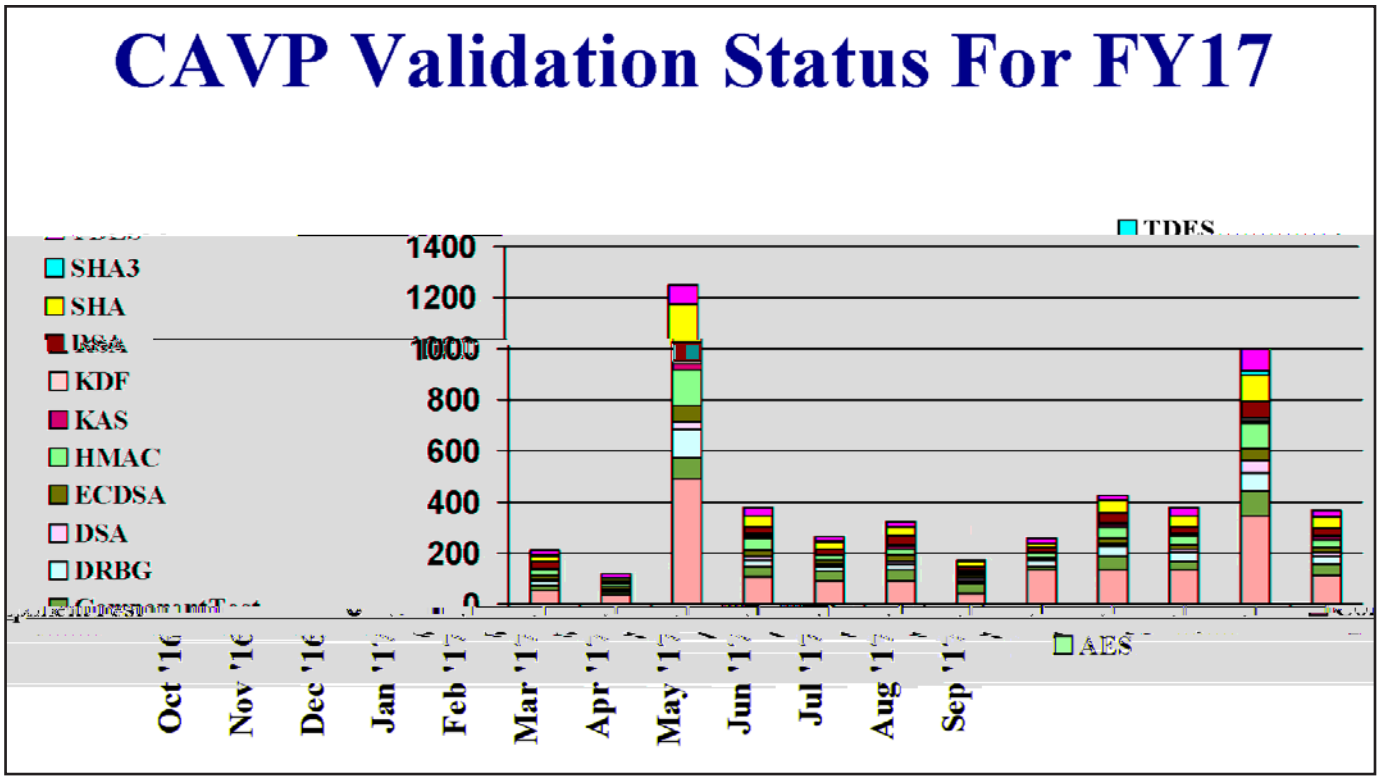


Figure 21: CAVP Validation Status for FY 2017

CAVP Validated Implementation Actual Numbers

Updated As: Friday, November 03, 2017

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	1179	226	0	99	320	164	355	32	35	80	243	396	0	258	**3387**
FY2016	1357	329	0	125	339	214	422	50	32	23	305	463	0	303	**3967**
FY2017	1786	503	0	170	426	271	508	88	52	0	391	547	0	371	**5147**
Total	**8567**	**1422**	**331**	**1276**	**1656**	**1199**	**3180**	**268**	**154**	**1396**	**2508**	**3922**	**19**	**2773**	**28710**

Figure 22: Validated Implementation Actual Numbers

The CAVP issued approximately 5,000 algorithm validations in FY 2017, an increase of approximately 100 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.

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/groups/computer-security-division/security-testing-validation-and-measurement

CONTACT:

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

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

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 list to use in procuring and deploying validated cryptographic modules, and promote the use of those modules by industry and the public. The testing performed by independent third-party laboratories accredited by 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 the 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. A module may be a standalone product, such as a virtual private network (VPN) or smart card, or it could be a module embedded in many products, such as a cryptographic-based toolkit. As a result, a small number of modules may be incorporated within hundreds of products.

The theme for FY 2017 was modernization. As part of the launch of the new Computer Security Resource Center (CSRC) web site, the CMVP web pages were redesigned and now have a new look with additional functionality. The CMVP was automated to improve its validation processes, the Cryptographic Validation Program (CVP) Certification Exam was developed, and collaboration was continued with the Cryptographic Modules User Forum (CMUF) to publish new CMVP Implementation Guidance (IG).

The CMVP uses an automation system to manage the validation workflow. This automation continues to reduce the administrative overhead for the program allowing the staff to focus on addressing the technical needs of the community. The automated system tracks the status of each submission and identifies the order that the submission should be reviewed, based on when the submission was added to the CMVP queue. In FY 2017, the CMVP awarded 271 new certificates. Figure 23 displays the number of certificates that were issued by security level.

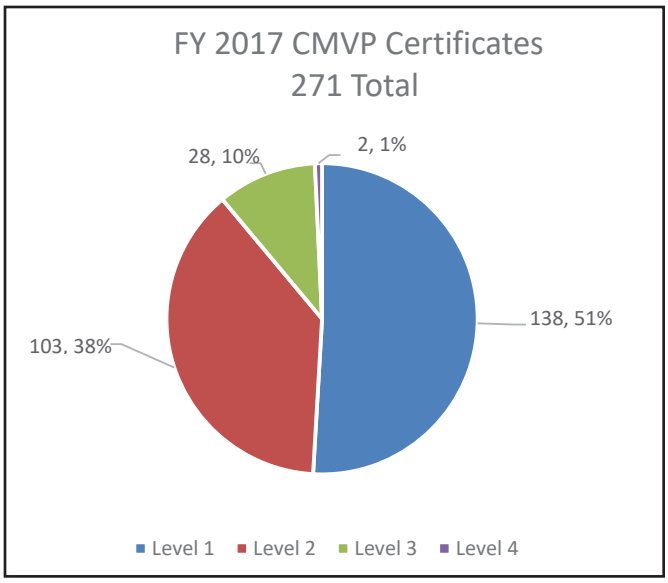


Figure 23: FY 2017 CMVP Certificates by Security Level

Initially, this system automated the creation and transmittal of billing invoices, but then was further enhanced to allow laboratories to submit those invoices in advance of the report submission. For laboratories and vendors who elect to take advantage of this, the amount of time that submissions wait in the queue prior to being assigned has been reduced, which in turn lessens the overall time to validation. This enhancement provides significant time savings and was achieved due to the continued collaborative effort between the CMVP and NIST Receivables.

In order to provide a greater transparency to the laboratories, the CMVP sends a weekly report to each laboratory providing a status of each of their submissions. The CMVP provides those reports to apprise the laboratories of the current state of each submission along with their respective payment status. This has mitigated the number of status requests that need to be addressed by the CMVP.

Since August 2015, the CMVP produces a separate Implementation Under Test (IUT) list from the Modules In Process (MIP) list. The IUT list is merely provided as a marketing service for vendors. However, to encourage this list to be kept up to date, the CMVP implemented a new policy to drop IUT entries that are greater than 18 months old. The MIP list continues to reflect the status of the current work that is actively in the validation process.

In February 2017, the CMVP adopted the five year Validation Sunsetting Policy that moved all FIPS 140-1 validation entries and all validations that were completed prior to February 1, 2012 from the Active Validation List to the Historical Validation List. This was done to ensure that modules on the Active Validation List are compliant with the latest standards and guidance. In January 2018, the CMVP will drop modules to the historical list that have not been validated within two years of report or billing submission, whichever occurred first. This is to encourage the completion of projects and to ensure that the MIP list reflects modules that are actively in the validation process.

In order to demonstrate proficiency in the technical areas addressed by Handbook 150-17, *NVLAP Cryptographic and Security Testing*, the CMVP activated the CVP Certification Exam in July 2017. This exam is now required as part of the initial and renewal accreditation process. The proficiency testing was previously handled by the NVLAP/CMVP technical assessors at the onsite audit, but is now being managed through a third-party testing facility. Each laboratory must have a minimum of two testers who pass the exam to be eligible for initial or renewal accreditation. The certification will remain with the individual tester making it easier to access the laboratory's overall competency, as its staff may change over time. In support of this effort, the CMVP also created a web site and user's guide that provides information on this new certification process.

In September 2017, the NIST CSRC launched a new website. In support of that effort, the CMVP updated its web pages to include both basic and advanced search capabilities. The basic search results in the list of all active validated modules. The more advanced search allows the user to search on specific fields and to retrieve historical and revoked certificates. For each validation, there are links provided to related files that direct the user to the module's security policy and to the applicable consolidated certificate. The consolidated certificates are generated once a month and include the individual validations that were completed within that particular month. The posting of the most current CMVP IG document was also separated from the archived versions that are still accessible for historical reference.

The CMVP has maintained the relationship with the CMUF by supporting the monthly CMUF general membership meetings and the CMUF working groups. The working groups are chaired by a member of industry and/or laboratory personnel. Each working group includes a representative from the CMVP. The current working group tasks include the Revalidation and Response to Common Vulnerabilities and Exposures (CVEs), ROM Integrity Testing in Constrained Devices, and Testing Equivalency. Working groups are dissolved once discussions on the topics are completed, and guidance is typically published.

In order to provide predicable support for vendors and laboratories needing guidance, the CMVP implemented a quarterly IG release process. New draft IGs and revisions to currently posted IGs are sent out once a month to the laboratories for comments. Vendors are encouraged to provide their feedback, so draft IGs are also posted on the CMUF Forum. The comments are adjudicated by the CMVP, and the finalized IGs are incorporated into the main IG document, which is posted quarterly on the CMVP web site.

For FY 2018, the CMVP 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. The CMVP will continue to:

- Invest in automation to streamline the validation process and improve review consistency,
- Strengthen its relationship with the CMUF by collaborating on new and improved technical guidance and programmatic issues, and
- Support the ICMC committee to continue strengthening the relationship with vendors and laboratories.

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/projects/cryptographic-module-validation-program/module-validation-lists
https://wsr.pearsonvue.com/nist-cmvp

CONTACT:

Ms. Beverly Trapnell
(301) 975-6745
beverly.trapnell@nist.gov

Automated Cryptographic Validation (ACV) Testing

The Cryptographic Module Validation Program (CMVP) was established on July 17, 1995 by NIST to validate cryptographic modules for conformance 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 24 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 progresses and cryptography becomes ubiquitous in the federal IT infrastructure, the plethora of cryptographic module validations has proven to outstrip available human resources for vendors, third-party testing laboratories and federal validators alike. As the number and complexity of modules to be validated increases, the existing methodologies face a limit on their ability to catch and eliminate all possible defects that could compromise the security. Testing is exceedingly long — well beyond typical product-development cycles across a wide range of technologies — yet costly and ineffective. 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.

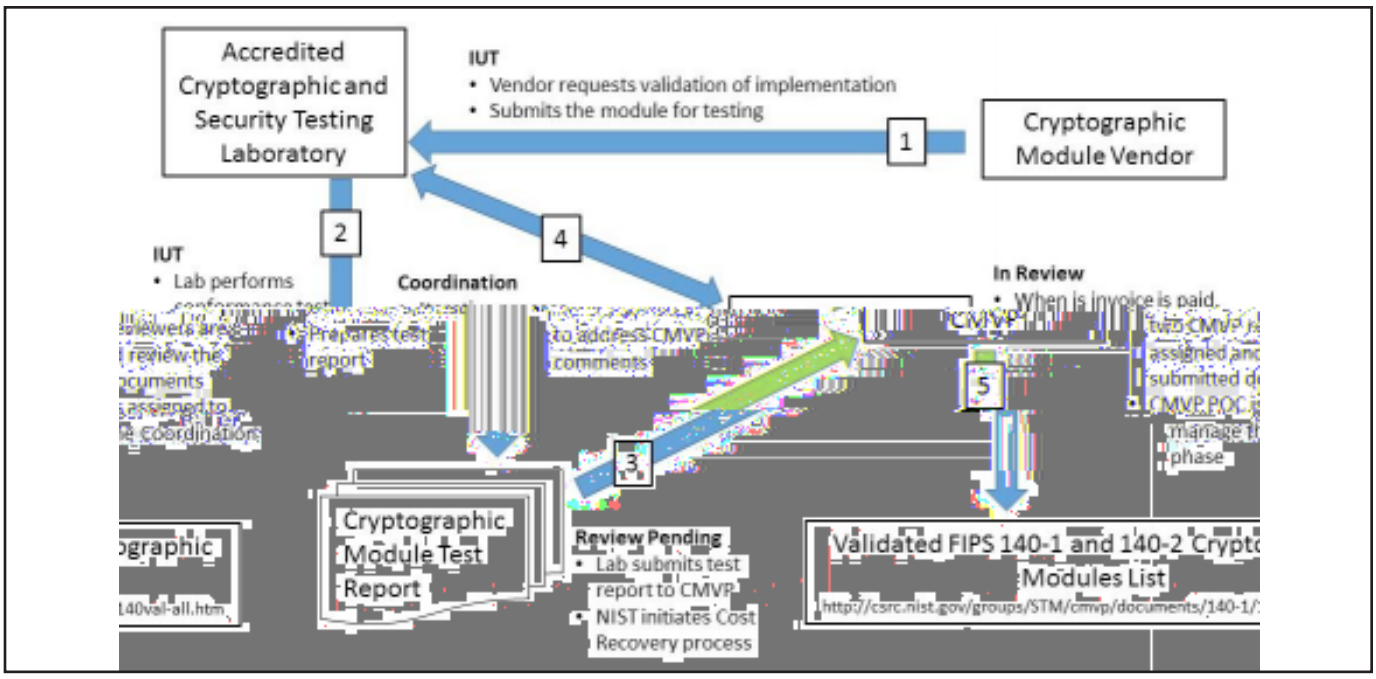


Figure 24: Current Validation Flow

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:

- 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 XML or JavaScript Object Notation (JSON) files containing logs from performed tests and the corresponding results – see 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.

The new structure of the CMVP is shown in Figure 25. It leverages automation through computer analysis of test results.

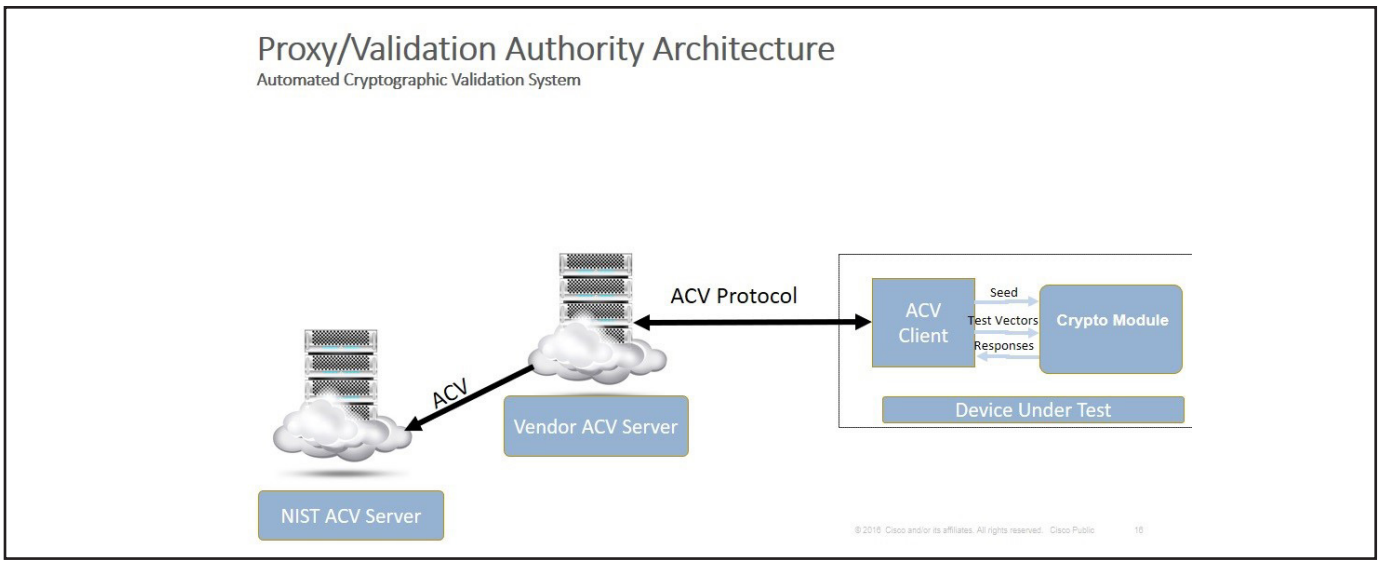


Figure 25: Updated CMVP Structure Leveraging Automation

Currently, the project is focused on completing the documentation of the technical approach for automating the algorithm testing and finalizing the implementation of the automated algorithm testing server. The team is also working on researching the approaches for automating the software module testing. The team working on this project, in collaboration with industry, established a demonstration algorithm testing server that is currently capable of testing over 30 algorithms (see https://demo.acvts.nist.gov/acvp/home). The work is progressing, and new algorithms are added to it on an ongoing basis. Eventually, this demonstration functionality will be transferred into the production server for algorithm validation testing. The team developed criteria for participation in the automated testing for commercial companies wishing to validate their cryptographic algorithm implementations. The criteria are positioned as an annex to NIST Handbook 150-17, *NVLAP Cryptographic and Security Testing*, which NVLAP uses to accredit laboratories. This criteria will be used, beginning in FY 2018, to establish a new testing scope for algorithm testing.

The project activities are structured by work areas in order for subject-matter experts to more narrowly focus on program needs and develop solutions:

1. Algorithm and Protocol Testing;
2. Cryptographic Module Testing,
    a. Software,
    b. Modules in cloud environments,
    c. Hardware; 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 FIPS 140 DTR requirements, and a selection of the best technical and feasible approaches.

CONTACT:

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

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.

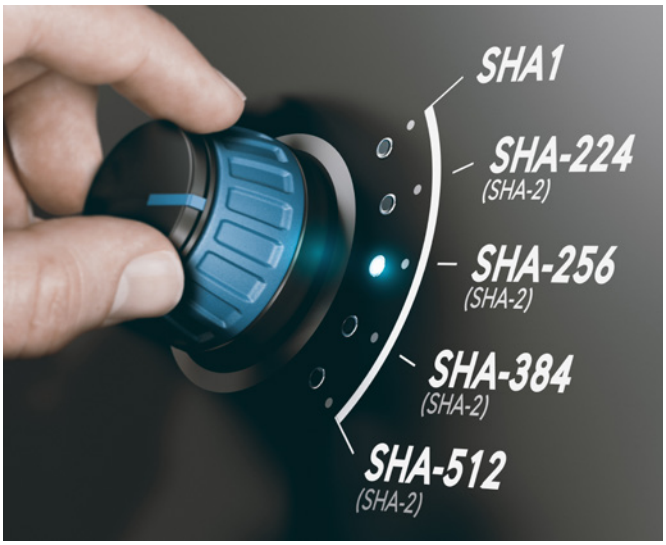
The conformance testing consists of a suite of validation tests for each approved cryptographic algorithm. These validation tests exercise the algorithmic requirements and mathematical formulas to assure that the detailed specifications are implemented correctly and completely. If the implementer deviates 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 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, CSD 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:



Credit: Shutterstock/Olivier Le Moal

Various Types of SHAs

TABLE 2: CRYPTOGRAPHIC ALGORITHMS & NIST TECHNICAL DOCUMENTS (FIPS & SPs)

CRYPTOGRAPHIC ALGORITHM/COMPONENT	FEDERAL INFORMATION PROCESSING STANDARD (FIPS), 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*

TABLE 2 (CONT): CRYPTOGRAPHIC ALGORITHMS & NIST TECHNICAL DOCUMENTS (FIPS & SPs)	
CRYPTOGRAPHIC ALGORITHM/COMPONENT	**FEDERAL INFORMATION PROCESSING STANDARD (FIPS), SPECIAL PUBLICATION (SP) OR OTHER REFERENCE DOCUMENT**
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 XOR–encrypt–XOR (XEX) Tweakable Block Cipher with Ciphertext Stealing mode	SP 800-38E, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Block-Oriented Storage Devices*
Key Wrapping	SP 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*
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 Internet Key Exchange (IKE) v1, IKEv2, Transport Layer Security (TLS), American National Standard (ANS) X9.63-2001, Secure Shell (SSH), Secure Real-time Transport Protocol (SRTP), Simple Network Management Protocol (SNMP), and Trusted Platform Module (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 Signwature Standard (DSS),* and Public Key Cryptography Standards (PKCS) #1 v2.1: RSA Cryptography Standard-2002
Component test – RSA PKCS#1 Probabilistic Signature Scheme (PSS) Signature Generation of encoded message EM (This component test verifies the RSASP1 function.)	SP 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography,* August 2009, Section 7.1.2

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

- SP 800-38G, *Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption*;
- SP 800-56C, *Recommendation for Key Derivation through Extraction-then-Expansion*;
- SP 800-132, *Recommendation for Password-Based Key Derivation Part 1: Storage Applications*; and
- SP 800-56A Revision 2, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*.

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 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, Red Hat Enterprise Linux, and Apple Mac OS 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 26 illustrates the SCAP 1.2 Validation Process.

Credit: Shutterstock/Rawpixel.com

Computer monitor displaying that a product has been tested.

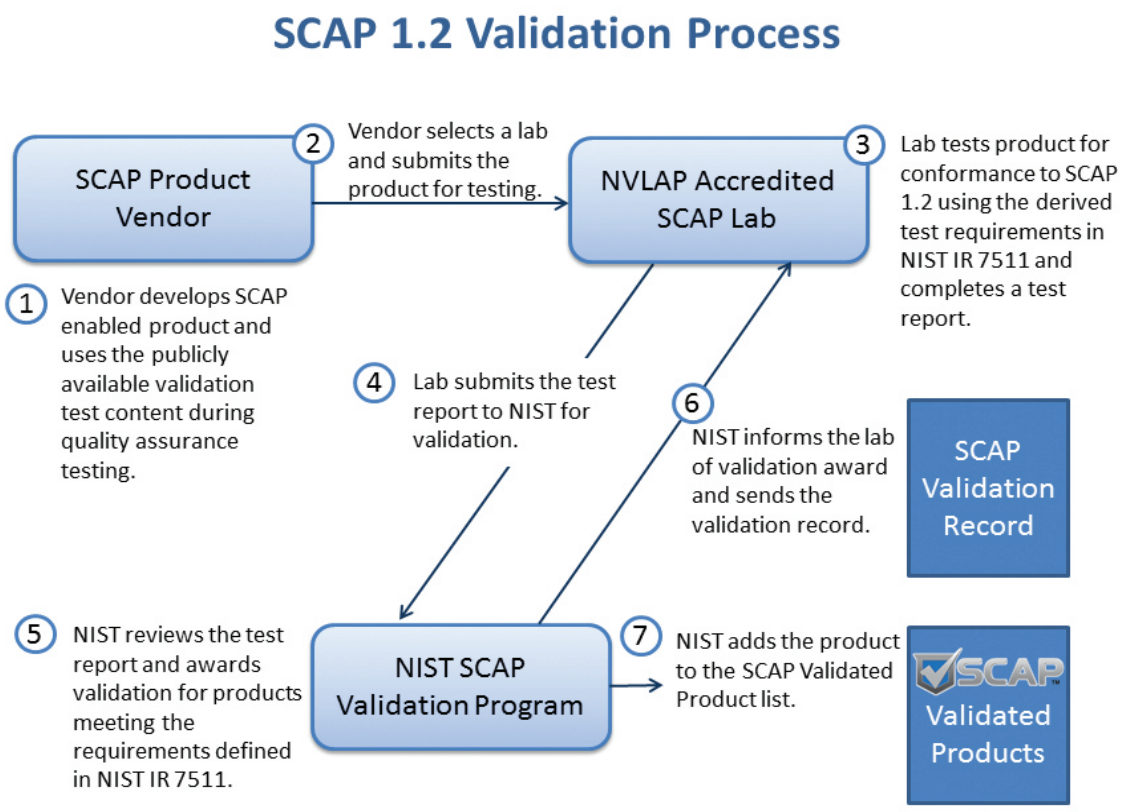


Figure 26: SCAP 1.2 Validation Process

All resources and information necessary for preparing products for SCAP 1.2 validation are published on the SCAP Validation Program web page (see https://scap.nist.gov/validation). The most current NISTIR 7511 revision, as well as SCAP capabilities and supported platforms, are available on the home page (see https://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. SCAP validated products may be used to process SCAP data streams for use cases such as checking compliance of target systems to a configuration checklist.

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 2017, NISTIR 7511 was updated in preparation for testing conformance to SCAP 1.3, and the validation test content was updated to include test coverage for SCAP 1.3 and support for new platforms. Support for Microsoft Windows 10 and Mac OS 10.11 was released in FY 2017; updates for SCAP 1.3 will be released in FY 2018.

Vendors continued to benefit from the openly available SCAP validation test suite reference material. Access to the validation test suite enables vendors to test products during development and provides a means for verifying SCAP conformance after operational products are patched. Through the use of the reference materials, vendors that market their products to federal agencies may better prepare for formal validation testing with NVLAP accredited laboratories. Vendors focused on the

critical infrastructure, and for which formal validation testing may not be required, have access to reference material that ensures that scanning products are correctly processing SCAP content. Approximately 86 % of configuration scanning products are SCAP-validated, and SCAP product vendors continue to engage with the SCAP Validation Program on new releases of the validation test content. 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 2018, NISTIR 7511 for SCAP 1.3 and the associated validation test suite reference material will be released. In addition, the program will continue to add support for new platforms (i.e., Windows Server 2016 and Mac OS 10.12). The program will continue to collaborate with vendors, laboratories, and the Security Automation team on updating validation resources in a meaningful way that meets the needs of federal agencies and the critical infrastructure. Coordination with the Security Automation team ensures that validation resources are developed and released in conjunction with new releases of SCAP.

FOR MORE INFORMATION, SEE:

https://scap.nist.gov/validation/

CONTACT:

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

(Editors' Note: Melanie Cook supported this program until her recent departure from NIST.)

IDENTITY AND ACCESS MANAGEMENT

NIST Personal Identity Verification Program (NPIVP)

The objective of the NIST Personal Identity Verification Program (NPIVP) is to validate Personal Identity Verification (PIV) products for conformance to the specifications in FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors.* There are three companion technical documents:

1. SP 800-73, *Interfaces for Personal Identity Verification*;
2. SP 800-76, *Biometric Specifications for Personal Identity Verification*; and
3. SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*.

The two main products are: the PIV Card Application and the PIV Middleware. The guidelines for performing the conformance tests for these products are themselves outlined in two technical documents (SP 800-85A, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-4 Compliance)*, and SP 800-85B, *PIV Data Model Test Guidelines*); they specify a two-step process that first involves the development of Derived Test Requirements (DTRs) and then the actual test procedures. To implement these tests and to generate conformance test reports, CSD also developed test modules for testing the PIV card application and PIV middleware. These modules were provided to NPIVP test facilities for testing and certifying the vendor submissions in the two PIV product categories. NPIVP test facilities are Cryptographic and Security Testing (CST) Laboratories that were accredited by the NVLAP. NPIVP also assisted NVLAP in the accreditation of laboratories by developing technology-focused assessment criteria. An additional software module to perform conformance testing for the PIV data model was also developed by CSD to enable GSA to provide a toolkit to agencies for testing fully personalized PIV cards prior to card issuance.

FIPS 201 specifies the architecture and technical requirements for the PIV cards. Since the start of the NPIVP, FIPS 201 has undergone two revisions and the companion technical documents even more revisions. The two test guidelines documents have also been updated to be consistent with the specification documents. The NPIVP team was fully involved in the review, analysis and development of these revisions of specification documents and have also ensured that these revisions are fully reflected in the two test guidelines documents as well as in the test software modules. The latest versions of all documents (as of September 2017) with their URLs, as well as the URL

for the list of accredited NPIVP labs are given below:

Specification Documents:

- FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors* – (see https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf)
- SP 800-73-4 Parts 1-3, *Interfaces for Personal Identity Verification* (see https://doi.org/10.6028/NIST.SP.800-73-4)
- SP 800-76-2, *Biometric Specifications for Personal Identity Verification* (see https://doi.org/10.6028/NIST.SP.800-76-2)
- SP 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification* (see https://doi.org/10.6028/NIST.SP.800-78-4)

Test Guidelines Documents:

- SP 800-85A-4, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-4 Compliance)* (see https://doi.org/10.6028/NIST.SP.800-85A-4)
- Draft SP 800-85B-4, *PIV Data Model Test Guidelines* (see https://csrc.nist.gov/CSRC/media/Publications/sp/800-85b/4/draft/documents/sp800_85b-4_draft.pdf)

List of Accredited NPIVP Labs

As of September 2017, there are six accredited NPIVP labs (see https://csrc.nist.gov/projects/nist-s-personal-identity-verification-program/testing-facilities).

During FY 2017, NPIVP did a major redesign of the test software modules. The three software modules for PIV card application conformance testing, PIV Middleware conformance testing and PIV data model conformance testing were all integrated into a single comprehensive toolkit to eliminate redundancies and inconsistencies in software codes performing the same functionality and to make the maintenance of the overall toolkit much easier. Further tests pertaining to different card interfaces (Contact, Contactless, Secure Messaging and Virtual Contact) for the same command were grouped together for easy accessibility. The redesigned test toolkit (now called the SP 800-73-4 PIV Test Runner for PIV Card Applications, Middleware and Data Model) has been made freely available to the public and can be downloaded at https://csrc.nist.gov/Projects/NIST-Personal-Identity-Verification-Program/Software-Downloads.

NPIVP's PIV Card Application Validation List is available at https://csrc.nist.gov/Projects/NIST-Personal-Identity-Verification-Program/Validation-Lists/PIV-Card-Application-Validation-List.

The PIV Middleware Validation List is available at https://csrc.nist.gov/Projects/NIST-Personal-Identity-Verification-Program/Validation-Lists/SP-800-73-4-PIV-Middleware-Validation-List.

During FY 2017, five PIV card application products were certified and validated.

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)

Figure 27: 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*, the following NIST standard was developed, FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*. FIPS 201 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 ITL, this work is a collaborative effort of the CSD and the IAD. CSD activities in FY 2017 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 initiating implementations of the credential on mobile devices. CSD performed the following activities during FY 2017 in support of HSPD-12:

- Coordinated with the revision team in the ACD to update SP 800-63, titled *The Digital Identity Guidelines*, and ensured close alignment with the PIV Standard in areas of enrollment, identity proofing, authentication and credential lifecycle management.
- With industry CRADA partners, built sample solutions at the NCCoE to demonstrate the issuance and use of PIV Credentials on mobile devices using commercial technologies. For more information visit https://nccoe.nist.gov/projects/building-blocks/piv-credentials.
- Coordinated cybersecurity-related updates with vendors, departments and agencies to ease migration to stronger cryptography for identity credentials and for a PIV system that produces, manages, and uses the credential -- to include the sunset of the Triple Data Encryption Algorithm (TDEA), the upgrade to Deterministic Random Number Generator (DRBG).

In FY 2018, CSD will continue to focus on updating the relevant publications associated with FIPS 201-2, including 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:

https://csrc.nist.gov/projects/piv

CONTACTS:

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

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

Access Control and Privilege Management

With the advance of the 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. This project is intended to provide practical and conceptual guidance for these issues.

In FY 2017, the following activities were accomplished:

- Published a conference paper: *Access Control for Distributed Processing Systems: Use Cases*

and General Considerations, which discussed fundamental requirements as well as some general access control implementations for distributed system environments.

- Continued working on attribute considerations for access mechanism implementation; the results will be 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 2018).
- Added new functions in NIST's Access Control Policy Tool (ACPT) for efficiently combining access control policies for systems that require multi-policy access control.
- Researched a general Access Control (AC) framework for distributed systems, including Big Data, Cloud, IoT, and the Smart Grid.

In FY 2018, 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 AC 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 AC 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 28 illustrates the application of AC and privilege management within and among organizations.

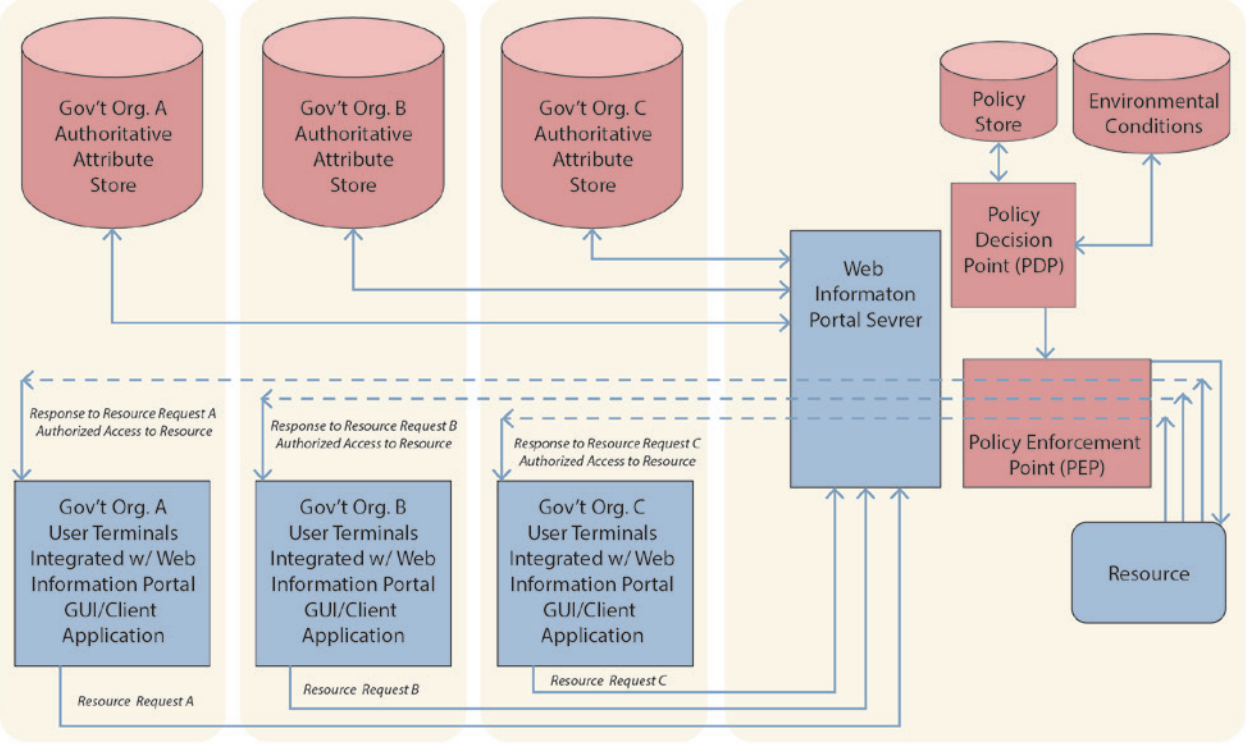


Figure 28: Access Control and Privilege Management

CONTACTS:

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

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

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

Conformance Verification for Access Control Policies

Access control (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 AC policies is often a challenging problem. Often, a system's privacy and security are compromised due to the misconfiguration of AC 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 intended properties 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 AC 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 AC model is correctly expressed in the AC policies, and whether the properties are satisfied in the model.

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 but by multiple rules that conflict. 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 ACPT, shown in Figure 29, 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 2017, CSD accomplished the following:

- Published SP 800-192, *Verification and Test Methods for Access Control Policies/Models*, an article, *Access Control Policy Verification* in *IEEE Computer*, and a conference paper, *Differentiation Non-Isomorphic Graphs for Graph Analytics*;
- Enhanced the capability of ACPT by including additional functions for the specifications of subject inheritance, separation of duty requirements, and better user interfaces for policy model specification;
- Enhanced the usability and fixed bugs of the ACRLCS (the Access Control Rule Logic Circuit Simulation System) to provide more policy composing and user interface capability for policy fault detection;
- Supported two Small Business Innovation Research (SBIR) Phase II projects for the access control tool and embeded function developments; and

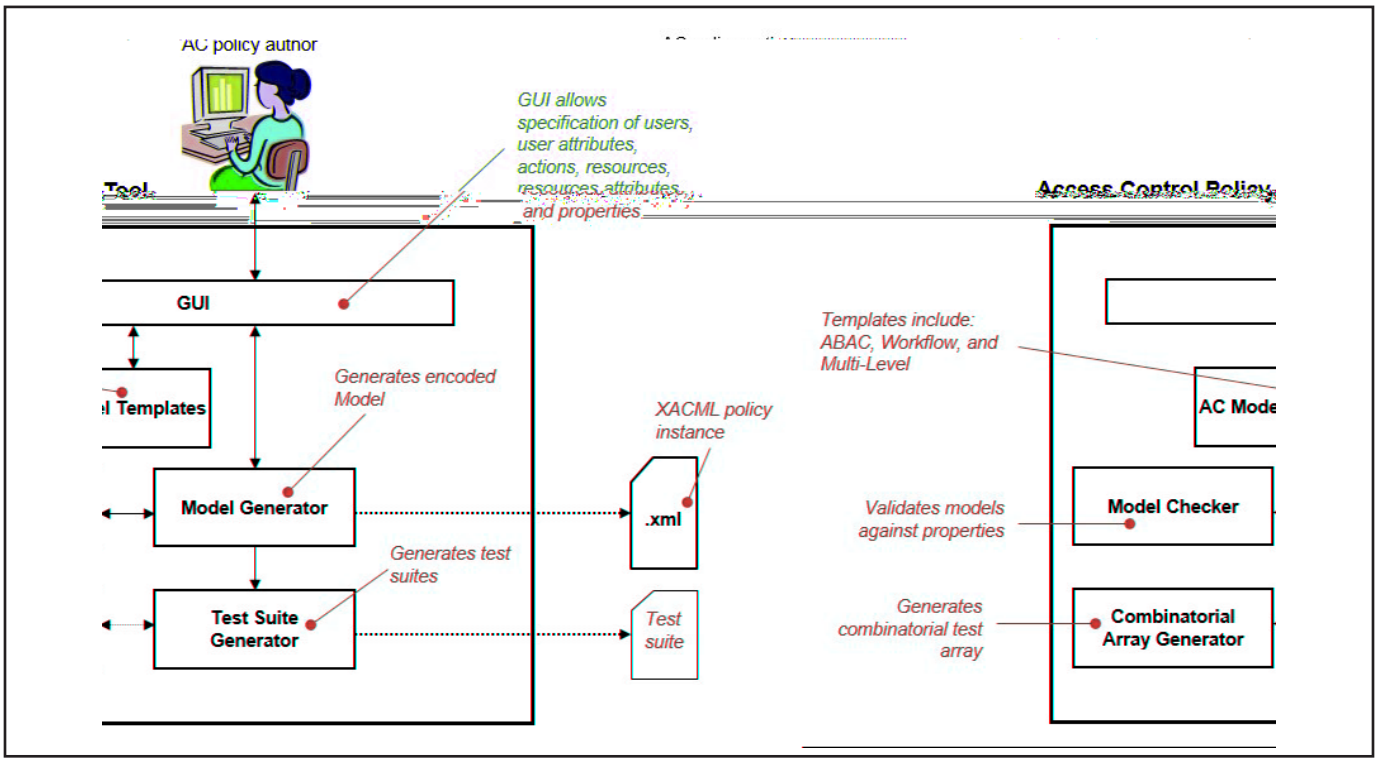


Figure 29: Access Control Policy Tool (ACPT)

- Worked with industrial and academic rganizations 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 475 users and organizations.

In FY 2018, CSD is planning to conduct further research on efficient testing technology, develop new capabilities, and to enhance the performance of the ACPT and ACRLCS.

Figure 29 shows the system architecture of the NIST ACPT, which allows access control policy authors to compose, verify, and test access control policy implementation.

Figure 30 provides an example of access control rule implementation in ACRLCS, which allows the online detection of access control rule composition faults.

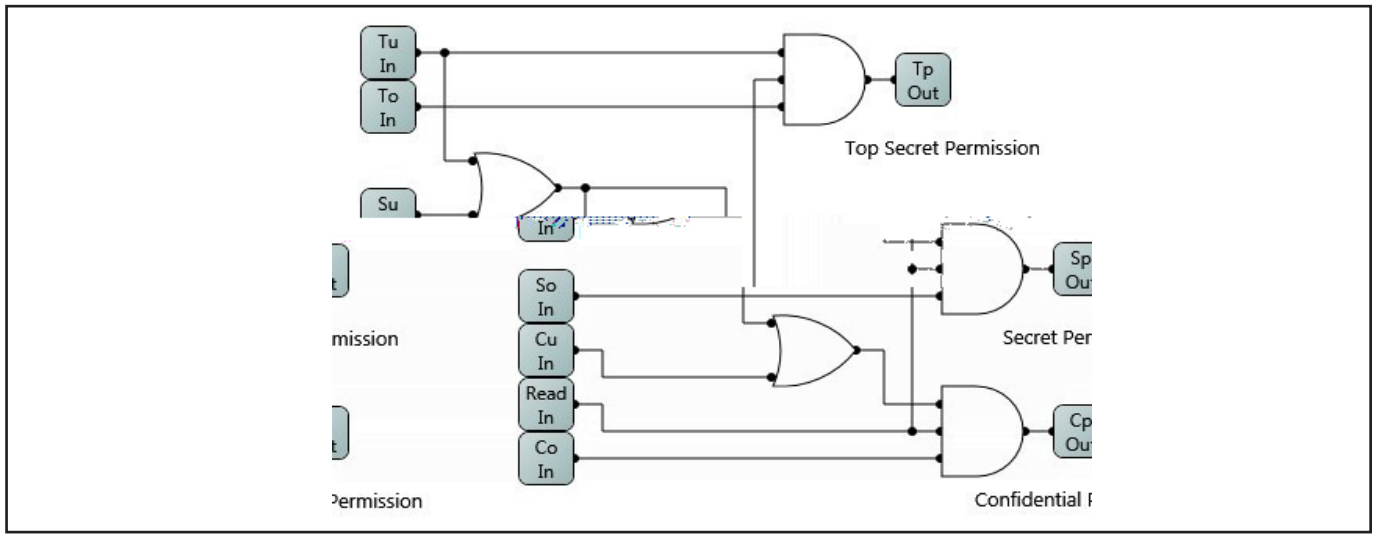


Figure 30: Access Control Rule Implementation

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, Multi-level, 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:

https://csrc.nist.gov/projects/access-control-policy-tool

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 Control (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 31 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 2017, the project team:

- Published the book *Attribute-Based Access Control* by Artech House. The book contains discussions covering almost all aspects of ABAC;
- Published a conference paper: *Verification of Resilience Policies that Assist Attribute Based Access Control*. The paper presents research results of access privilege blocking and privilege leaking; and
- Worked with government, industry and academic organizations in exploring diverse models (e.g., Next Generation Access Control - NGAC) and applications (e.g., distributed systems: Cloud, Bigdata, IoT applications) of ABAC.

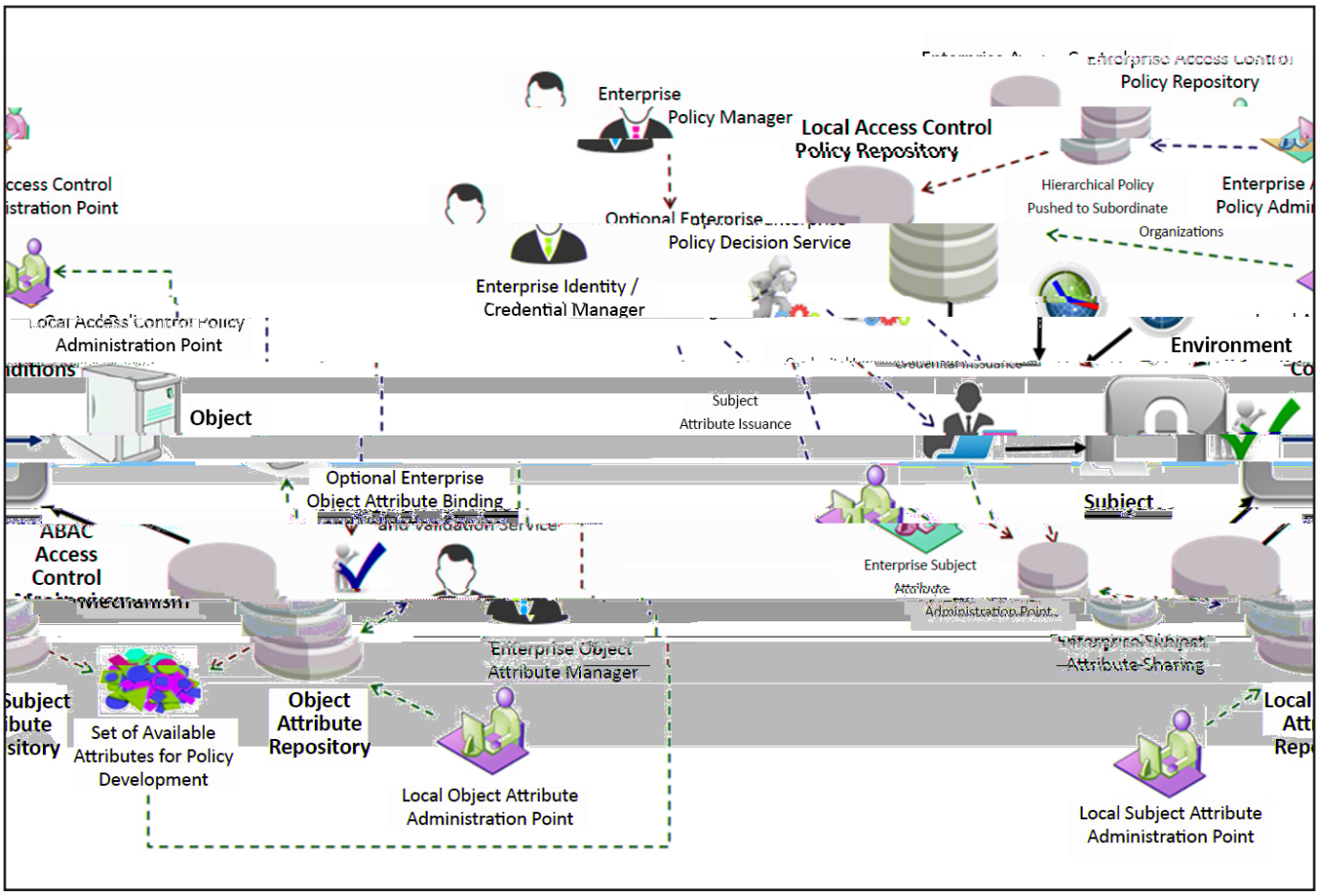


Figure 31: ABAC Access Control Mechanism Chart

In FY 2018, CSD will continue the research of ABAC formal models, as well as the 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:

- 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:

https://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 Program

By promoting the government and commercial adoption of privacy-enhancing, secure, interoperable, and easy-to-use digital identity solutions, ACD works alongside its partners to drive trust, convenience, and innovation in the marketplace of identity solutions (see https://www.nist.gov/itl/tig). ACD is committed to advancing measurement science, technology, and standards adoption to improve digital identity for individuals and organizations alike.

In FY 2017, the Trusted Identities Program was a key participant and driving force in the digital identity arena for NIST's National Cybersecurity Center of Excellence (NCCoE). Many identity-related projects initiated at the NCCoE leveraged the technical expertise and experiences of, and the foundational guidelines and practices issued by, ACD and NIST's broader identity program.

Through these collaborative efforts, projects this year focused on driving the adoption of trusted identities through digital identity standards, including for federal agencies. NIST also engaged the community on standards and guidelines development, including issuing SP 800-63-3, *Digital Identity Guidelines*, collaborating with other countries to advance high-assurance online identity standards, and participating in the OpenID Foundation and Fast Identity Online (FIDO) Alliance.

ACD also focused on building trust in digital identity technologies by advancing measurement science in the identity space—which included measuring the strength of authenticators and evaluating attribute metadata. The team also continued work with numerous external partners through trusted identities pilots, seeding the market with innovative technologies and providing solutions.

Updated Digital Identity Guidelines

In June of 2017, ACD finalized the latest revision to SP 800-63-3, which covers digital identity from initial risk assessment to deployment of federated identity solutions. Digital identity in both agencies and the market place have changed dramatically since the publication's last revision in 2013; the latest update was designed to give agencies more options and to align with international standards. One of the most significant updates is replacing levels of assurance with three individual components of the digital identity flow for more flexibility in design and operations: the identity, authenticator, and federation assurance levels. Identity proofing was also updated to further mitigate the potential for mass breaches of personal information.

Over the course of a year, the document evolved with the help of the community. For this revision, GitHub was used to interact in near-real-time with the community and received a tremendous response: over 1,400 comments were submitted, and the web version of the publication drew over 74,000 unique visitors between May 2016 and May 2017. ACD will continue to use this approach in the future during the development of new volumes and document revisions.

International Standards Alignment

ACD, the United Kingdom Cabinet Office, and the Canada Treasury Board have been collaborating to compare national frameworks for identity assurance with the intention of creating a broad and competitive global market for identity solutions and enabling cross-border credential interoperability. Building on recent updates to guidance documents like NIST's SP 800-63-3 and the UK's Good Practice Guides, the group made several recommendations for the International Organization for Standardization's (ISO's) suite of identity standards. These recommendations included the development of a new standard that provides an overall approach to identity and authentication risk management and assurance; organizations could leverage this when developing their models for assessing and managing identity-based risks and threats.

The group also recommended refocusing ISO/IEC 29115, *Entity Authentication Assurance Framework,* to address authentication threats and risks exclusively. These updates should contain a threat model, controls and mitigations, and guidance on how these can be combined to achieve defined risk management outcomes for authentication events.

NIST staff members served as the Federal Government lead for all activities in the (Fast IDentity Online) FIDO Alliance, which focuses on creating

strong authentication specifications to create an identity ecosystem. During 2017, ACD participation included active membership and contribution in technical and privacy working groups, as well as international plenary participation in Hong Kong, Vancouver, Madrid, and Sydney.

Additionally, ACD supported standardization efforts including iGov (see https://openid.net/wg/igov). The iGov is working toward an OpenID Connect specification that will enable users to authenticate and share consented attribute information with public-sector services across the globe. The resulting profile will enable standardized integration with public-sector relying parties (RPs) in multiple jurisdictions.

Authenticator Strength of Function

NIST is working to produce a framework for evaluating and comparing the strength of authentication solutions, starting with the Strength of Function for Authenticators – Biometrics (SOFA-B). The team began with a focus on biometrics, due to the increased availability of biometric solutions in the consumer space and the need for improved security guidance regarding the use of those solutions as authenticators. The end goal is a framework to assess and combine authentication technologies, as well as to compare biometrics' effectiveness to that of passwords and other authenticators. Using the SOFA-B framework, RPs will be able to determine the overall strength of biometric authentication, considering matching performance, presentation attack detection, and the effort required to break – or spoof – a system.

With the draft of NISTIR 8112: *A Proposed Schema for Evaluating Federated Attributes*, the TIG aims to give RPs greater insight into how attributes assist with risk-based business decision-making. RPs can examine this metadata and determine if they have the confidence they need in the attribute value before making an authorization decision. This NISTIR is being treated like an implementers' draft, an approach focused on real-world implementation results and lessons learned before finalizing the document. ACD plans to advance SOFA-B and attribute metadata efforts to their next stages in FY 2018.

Innovative Digital Identity Solutions

ACD has advanced trusted digital identity solutions by building partnerships that stem from the trusted identities pilots. These pilots develop and deploy technology, models, and frameworks that would not otherwise exist in the marketplace, and have impacted more than 8.8 million individuals to date. In FY 2017, the pilots made remarkable progress: the 24 projects now involve more than 190 partner organizations across 12 sectors — including the development or deployment of 16 multi-factor authentication solutions.

In FY 2018, NIST, through the NCCoE, will fully integrate identity management standards, best practices, and technical approaches into projects that are foundational to the work of the NCCoE and many of its stakeholders and projects, including the Internet of Things. The project will also continue to advance the digital identity marketplace by collaborating with partners on measurement science, technology, and standards adoption, and develop guidance to meet today's digital identity needs.

FOR MORE INFORMATION, SEE:

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

CONTACTS:

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

Ms. Kristina Rigopoulos
(202) 309-4791
kristina.rigopoulos@nist.gov

(Editors' Note: Paul Grassi supported this program until his recent departure from NIST.)

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 has the potential to 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 will implement software systems to solve challenge problems using software development tool chains ("toolchains") of their own choosing, within specified time periods. The toolchains will be free to 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 will apply 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 will 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 will seek to show that wide-scale improvements in the overall security of software products can be realized without sacrificing a time-to-market goal. The competitions, which will be open to all interested parties, will aim to provide consistent application and measurement of commercial and research software development, composition, and reuse techniques.

In FY 2017, CSD personnel documented the Toolchain Infrastructure (TCI) in a collection of documents that included a concept of operations, system design specification, and administrator's and users guides. These documents helped inform the development of a python-based prototype of the TCI. The prototype development effort included automated unit test scripts for the TCI and the configuration and deployment of the TCI hardware. The team also refined a selected challenge problem by updating the problem descriptions, requirements, and test cases; and developed an exemplar challenge problem solution in python.

In FY 2018, CSD plans to complete the development and testing of the TCI prototype. The team will enhance the prototype to further improve its reliability and reproducibility, perform extensive testing of the TCI, and publicly announce the first toolchain competition.

CONTACTS:

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

Mr. Christopher Johnson
(301) 975-3247
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, and private behaviors as well as many

other attributes associated with quality. Privacy is particularly important because IoT-based systems will likely produce huge amounts of data as a result of sensing and surveillance. 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.

In July 2016, NIST released SP 800-183, *Networks of 'Things'*, which addressed the question: "What is the science, if any, underlying IoT?" After releasing that document, NIST has begun to look at how to apply the principles in the document in a practical setting, with a focus on healthcare. NIST has also looked at the security and privacy of virtual assistants, and how a network of things with low inherent testability can be tested.

Future work in this area will refine the definitions of the five core networks of things building blocks as presented in SP 800-183. For example, instead of considering all temperature sensors as equal, NIST will create categories of sensors for various applications and vertical domains. Furthermore, a small IoT lab to test "low-energy" devices is being architected. In addition, NIST plans to present these results in Revision 1 of SP 800-183, which are expected to be produced in by the end of 2018.

FOR MORE INFORMATION, SEE:

SP 800-183, *Networks of 'Things'*,
https://dx.doi.org/10.6028/NIST.SP.800-183
https://www.nist.gov/topics/internet-things-iot

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, *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 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 2017, focused on developing the guidance for applying a risk-based approach to cloud adoption and the guidance for leveraging the NIST Cybersecurity Framework in the process of architecting a cloud-based system secured with SP 800-53 Revision 4 security and privacy controls.

During FY 2017, NIST also researched the security challenges encountered when leveraging application containers and microservices for the implementation of cloud-based federal information systems, along with the impact on the system's security posture. Details regarding the latest projects are provided below.

CSD Role in the NIST Cloud Computing Program

During FY 2017, 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 2017, 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 initially focused on providing 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. As SP 800-37 underwent revision in late FY 2017, and is anticipated to be finalized in early FY 2018, the draft of SP 800-173 will be updated to reflect all changes incorporated in the SP 800-37 Rev. 2 and will be posted for public comment after publication of SP 800-37 Rev. 2.
- NIST Draft SP 800-174, *Security and Privacy Controls for Cloud-based Federal Information Systems*. This document provides a methodology that leverages the NIST Cybersecurity Framework (CSF) to architect a cloud-based information system and to identify security controls deemed necessary to implement in order to secure the system. The document will be available for public comment in the first quarter of FY 2018. The document will be accompanied by a tool, Cloud Security Architecture Tool (CSAT), that implements the methodology described in SP 800-174 and allows users to customize their data and tailor their security controls. The tool repository is available at: https://github.com/usnistgov/CloudSecurityArchitectureTool.

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, researched the security challenges encountered when leveraging application containers and microservices for the implementation of cloud-based information systems. Based on this research, ITL will publish (in early FY 2018) the NIST Interagency Report (NISTIR) documenting the findings and will provide recommendations based on the 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 SP 500-299: *Cloud Security Reference Architecture* and NISTIR 8006, *NIST Cloud Computing Forensic Science Challenges*. 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 SP 500-293, *U.S. Government Cloud Computing Technology Roadmap*.

CSD staff co-chaired several significant cloud computing efforts in 2017:

- Co-Chaired the NIST Cloud Computing Security Working Group and led the working group on the development of the NIST research on Application Containers and Microservices – security challenges and

best practices. The result of this effort will materialize in FY 2018 into the development of a NIST Interagency Report and a NIST Special Publication.

- Co-Chaired the NIST Cloud Computing Forensic Science Working Group and led the development of SP 800-201, *Cloud Forensics Reference Architecture*, which is currently in progress.

- 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 2018, 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/itl/cloud

CONTACT:

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

Fog Computing

Ubiquitous deployment of smart, interconnected devices is estimated to reach as high as 50 billion units by 2020. This exponential increase is fueled by the proliferation of mobile devices (e.g., mobile phones and tablets), smart sensors serving different vertical markets (e.g., smart power grids, autonomous transportation, industrial controls, smart cities, wearables, etc), wireless sensors and actuators networks. New concepts and technologies are needed to manage this growing fleet of Internet of Things (IoT) devices in a manner that ensures minimal latency across a distributed and decentralized model.

Researchers working with system and network engineers are continually developing innovative solutions to fill the technological gaps. Many of these solutions or computational paradigms have begun to be referred to as *fog computing*, *mist computing, cloudlets,* or *edge computing*. Lacking broad consensus on the distinction among these concepts, NIST facilitated an effort to better define these topics to help facilitate meaningful conversations among practitioners and researchers.

During FY 2017, NIST collaborated with the IoT community to develop SP 500-325, *Fog Computing Conceptual Model*. This publication provides the conceptual model of fog computing and its subsidiary concept, *mist computing*, and identifies these concepts in relation to *cloud computing*, *cloudlets*, and *edge computing*.

The fog computing research will continue in FY 2018 with the development of the draft of SP 800-199, *Security and Privacy Controls for Fog-based Information Systems*. This document, also referred to as the *fog computing overlay*, will identify the security and privacy controls specific to fog computing ecosystems, allowing users of this computational model to build resilient and survivable standalone fog computing environments that are more resistant to penetration attacks and are capable of limiting the damage from attacks when they occur.

CONTACTS:

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

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

NIST Cybersecurity for IoT Program

NIST's Cybersecurity for IoT Program develops and applies standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. By collaborating among stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables innovation. (see https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program).

In FY 2017, during the nascent phase of the Program, the team focused on engaging and collaborating with stakeholders across government, industry, international bodies, and academia to understand the IoT threat landscape and determine whether there is stakeholder interest in NIST guidance for securing their IoT ecosystems. To this end, the Program hosted the IoT Cybersecurity Colloquium in Gaithersburg to better understand the overall threat landscape from the point of view of the community (see https://www.nist.gov/news-events/events/2017/10/iot-cybersecurity-colloquium). The presenters discussed specific security and privacy risks and NIST's role in supporting these areas. The team is currently drafting a NISTIR on the presentations, themes, and community feedback.

Additionally, NIST and DHS co-chair the IoT Task Group of the *Interagency International Cybersecurity Standardization Working Group* (IICS WG). The IICS WG established the Task Group to determine the present state of international IoT cybersecurity standards. The Task Group has 54 federal employee participants representing 13 agencies and will convene in early FY 2018 to determine the next steps for its draft report. If approved, NIST is prepared to take this document through the NISTIR process in FY 2018 to collect industry input on specific areas, such as market adoption and challenges associated with the adoption of existing standards.

In FY 2018, the Cybersecurity for IoT Program will continue collaborating with stakeholders as NIST begins drafting guidance for IoT security and privacy. As part of the drafting process, the team will hold town-hall meetings for input on discussion drafts. The document is intended to educate federal agencies on common high-level security and privacy risks for IoT, and to introduce practical risk management considerations for IoT product selection, deployment, protection, and operation.

Additional information regarding the broad portfolio of NIST activities for supporting secure IoT can be found on our program website.

FOR MORE INFORMATION, SEE:

https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

CONTACTS:

Ms. Kat Megas
(202) 441-1147
katerina.megas@nist.gov

Mr. Ben Piccarreta
(202) 802-1861
benjamin.piccarreta@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 extensions.

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) (see http://www.techstreet.com/standards/incits/499_draft?product_id=1827386). 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*). This standard has been updated and was in the process of formal publication at the end of FY 2017.

In addition, as of the end of FY 2017, the work on Project 2193-D had been submitted to ANSI as INCITS 525: NGAC Implementation Requirements, Protocols and API Definitions (NGAC-IRPADS), for approval for an initial public review.

The standard for Project 2195-D has been 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 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 issued the first version of the Policy Machine Web Services through GitHub as an open-source distribution to support widespread experimentation of web-based applications. The current version of the web services supports most NGAC functionality. In order to provide an example of web-based clients, CSD is planning to issue an administrative interface for policy management, which will also include a user interface with PIV authentication (if feasible) and some sample applications (e.g., email, file management, records management, document editor, workflow, etc.).

In FY 2018, CSD will continue improving the Web services version of the Policy Machine to include the remaining NGAC functionalities and more applications to provide different use cases to support the community's use of the Policy Machine.

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/projects/policy-machine/

CONTACTS:

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

Ms. Gopi Katwala
(301) 975-6182
gopi.katwala@nist.gov

Security for a Virtualized Infrastructure

The objective of this project is to focus on security concerns in virtualization technology; the project was started at a time when the technology was just beginning to gain traction in data centers used for supporting enterprise IT applications as well as for providing cloud services. An IT infrastructure can be looked upon as having five components or resources: Hardware, Operating System (OS), and Applications that collectively form a compute node, together with network and storage components that provide the function of interconnecting the computing nodes and supporting a persistent medium for storing data respectively. Any of these five resources can be virtualized by building an abstraction layer on top of it, facilitating efficient utilization of that resource by other components or resources as well as providing a degree of isolation among the utilizing components.

The earliest component to be virtualized was the hardware (ubiquitously referred to as Server Virtualization) through an abstraction layer (software module) called the Hypervisor. This gave rise to an architecture where multiple computing stacks (called Virtual Machines or VMs) each with a different OS can be run on a single physical host (called a virtualized host). To connect the various VMs residing in a single physical host, an approach to networking (called the Virtual Network) had to be implemented. The Virtual Network used the software analogs of

hardware network devices such as network interface cards (NICs) and switches. Thus, the Virtual Network (which was later extended to connect virtualized hosts themselves in addition to VMs inside a single virtualized host) became an integral part of the server virtualization infrastructure. From FY 2014 to FY 2016, this project focused on providing guidelines for the secure configuration and deployment of hypervisors and virtual networks.

The next component to be virtualized was the OS itself. The application component of the computing stack was packaged into multiple self-contained lightweight software elements called Application Containers. The abstraction of the OS itself was enabled by a software module called "Container Runtime". This form of virtualization brought in several new technology components involved in building containers, storing them in repositories (called registries) and deploying and managing them (through a process called orchestration) as logical groups (called clusters). The resulting computing stack with all these new components is shown in Figure 32 as the Container Technology stack.

With the increasing adoption of application container technology for deploying, managing and maintaining applications, NIST identified threats to components involved in supporting containers as well as the security countermeasures to mitigate the effect of those threats through SP 800-190, *Application Container Security Guide* (see https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf).

In FY 2017, building on the information in SP 800-190, this project examined potential security solutions that provide the necessary countermeasures as well as the kind of security assurance requirements that each solution should satisfy in accordance with NISTIR 8176, *Security Assurance Requirements for Linux Application Container Deployments* (see https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8176.pdf). Because security solutions for containers vary significantly based on

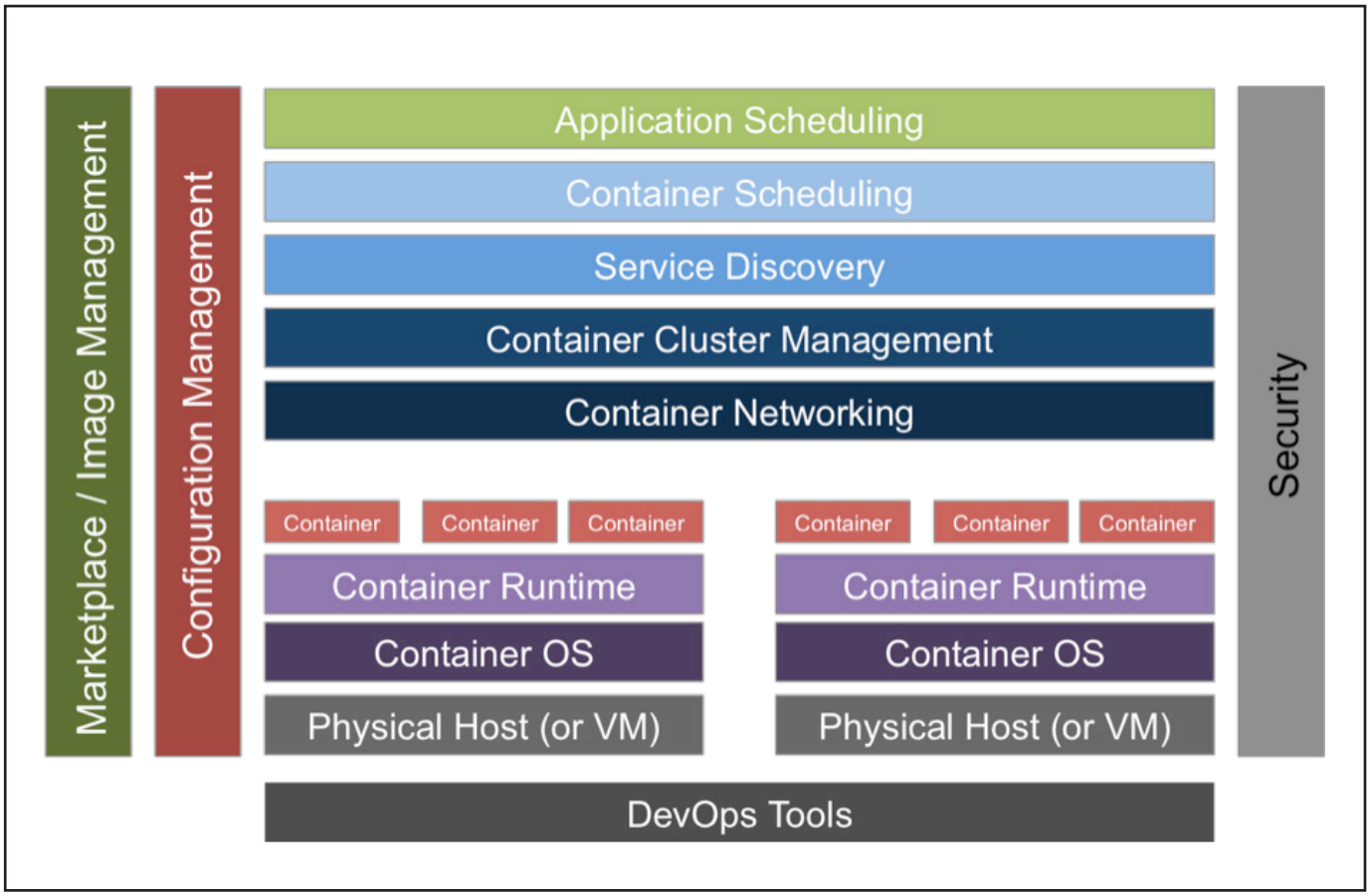


Figure 32: Container Technology Stack

the OS component (shown as Container OS in Figure 32) and because of their ubiquitous usage in container deployments, NISTIR 8176 focused on Linux OS-based environments. This decision enabled detailed security assurance requirements to be defined. Furthermore, the team recognized that there are multiple hypervisor products for server virtualization in current infrastructures. This observation led the team to modify previous security recommendations to improve countermeasures against potential threats to the hypervisor. These countermeasures are agnostic to any specific architecture of the hypervisor platform. The modified recommendations were published for public comment in the second draft of SP 800-125A, *Security Recommendations for Hypervisor Deployment* (see https://csrc.nist.gov/publications/detail/sp/800-125a/draft).

NIST contributed significant material that led to the creation of ISO/IEC Committee Draft 21878, *Security Guidelines for Design and Implementation of Virtualized Servers,* in April 2017. The draft was co-edited by a CSD computer scientist and drew from information in seven NIST conference papers and four technical publications regarding security for the virtualized infrastructure.

NIST recognizes that application container technology is being increasingly used to develop applications with microservices-based architectures. In FY 2018, this project plans to focus on security issues arising from technology components involved in that architecture. Developments in virtual networking and virtual storage technologies will be monitored to update our security recommendations for secure deployment of these technologies.

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 allowed, with whom the information may be shared, and how the information should be protected.

In October 2016, CSD published SP 800-150, *Guide to Cyber Threat Information Sharing*. This publication helps 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 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.

In May 2017, NIST conducted a Threat Intelligence Working Session as part of the Cybersecurity Framework Workshop. The working session provided an opportunity for attendees to provide comments on the use of cyber threat intelligence in the Framework, to help shape future enhancements to the Framework, and to share experiences regarding the use of cyber threat intelligence in the Framework. NIST used the feedback received during the workshop and the public review process as input when updating the Cybersecurity Framework Version 1.1 and its roadmap.

Throughout the year, CSD engaged with government, industry, and academia to research protocols, data models, and standards that enable cyber threat information sharing and support near real-time cybersecurity decision-making and security operations.

In FY 2018, CSD plans to continue to conduct research, prepare guidance, and take part in standards development activities that foster greater interoperability and increase the 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 recommendations have included the usage of passwords, biometrics, authentication hardware devices, and Public Key Infrastructure (PKI) solutions for enterprise authentication applications. Recently, CSD began researching 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 is in development that includes a detailed taxonomy and an assessment approach to aid in definitively comparing alternatives.

As the research matures, it is possible to draft a concept map (see Figure 33) to highlight key components. There are many intertwining aspects of authentication, such as the relationships with Identity Management and Authorization. As more of the aspects of authentication are identified and defined, better development and use of authentication is expected.

The structure of the authentication taxonomy (see Figure 34) to encapsulate current and emerging mechanisms continues to be refined as recent updates expand the diversity of mechanisms. The taxonomy includes entity authentication as a wide assortment of commonly used human-machine, machine-machine, and human-human methods, all of which are termed confirmation. Attestation is the term used for affirming expectations of objects.

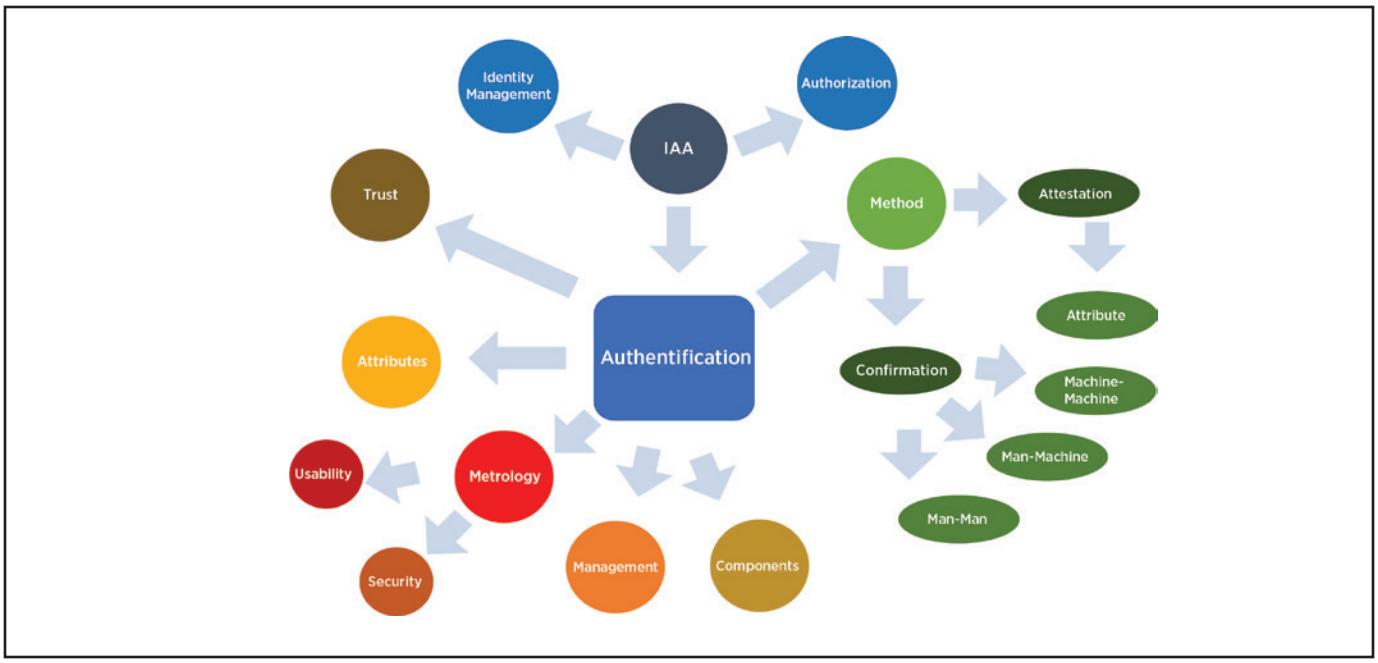


Figure 33: Draft Authentication Concept Map

The notional authentication ontology attempts to define an assessment framework that is useful for better understanding, comparing, and determining the appropriateness of authentication technologies to a specific use-case. The assessment framework separates attributes into security, usability, deployability, and manageability categories (see Figure 35). 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. To state the issue another way, there appears to be a relation between how much we must ask of the operator and how willing the operator is to support security rather than (mis)manage it.

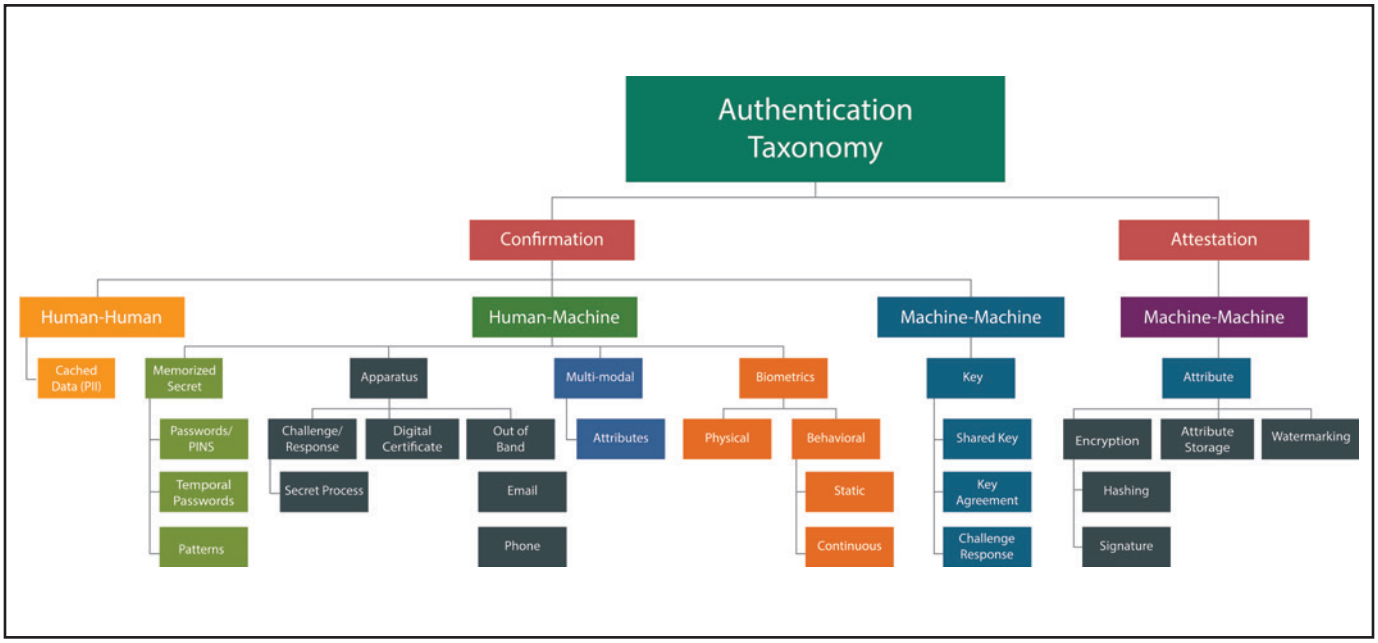


Figure 34: Draft Authentication Taxonomy

Figure 35: Suitability Framework for Authentication

Specific methods of assessment in these categories are not developed and are expected to be unique to each authentication mechanism and dependent on the environment. The assessment framework also includes integration with the programmatic categories of deployability and manageability. What is known is that these are unlikely to be reduced to a single value, but will have to be assessed across several independent constructs.

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. The goal is to move toward specifying independent strength requirements rather than specific implementation requirements. Upon completion of the NISTIR, work will begin on a suitability matrix that will aid the user in determining how best to apply and assess the assessment framework. Concerns as to the adoptability of this approach will be addressed. Additional work to identify interdependencies among identity management and authorization controls and requirements should aid in unifying the approach. As a clear assessment approach is defined, future identity management, authentication, and authorization process implementations can address vulnerabilities of individual or combined solutions.

CONTACT:

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

Cognitive-based Approach to System Security Assessment (CASSA)

The increase in information systems' complexity, due to the aggregation of broader-spectrum services and functionality within one system, challenges security professionals that are required to plan, analyze, design, implement and maintain systems compliant to various regulatory requirements supported by diverse sets of security controls, processes and procedures. For example, Veteran Affairs' hospital systems are often required to meet FISMA, Payment Card Industry (PCI) and Health Insurance Portability and Accountability Act (HIPAA) requirements simultaneously. Assessing and maintaining the security posture of such complex information systems through manual procedures leveraging paper-driven approaches is colossal, inefficient, and often unreliable.

NIST is researching methodologies for enhancing the security assessment and the near-real-time monitoring of complex systems. The team is leveraging cognitive approaches to provide continuous feedback by highlighting relevant threats, rendering security enhancements, or augmenting solutions to maintain/increase systems' security postures.

During FY 2017, NIST completed a feasibility assessment and created the project's research plan, identifying milestones and deliverables. In FY 2018 and subsequent years, the team will continue the Cognitive-based Approach to Security Controls Assessment (CASSA) by researching methods to:

- Identify the relationships between implemented security and privacy controls for a targeted information system;
- Analyze the implementation of the security and privacy controls, providing, as feedback, a rendered set of suggestions to enhance the security posture of the system;
- Identify documented and undocumented vulnerabilities relevant to the system;
- Identify the minimum-resistance penetration path into the system, providing, as feedback, rendered recommendations for mitigating the risk; and

- Perform continuous monitoring and analysis of the system, factoring in the above steps while providing rendered suggestions for system enhancements.

CONTACTS:

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

Dr. Dmitry Cousin
(301) 975-5727
dmitry.cousin@nist.gov

Open Security Controls Assessment Language (OSCAL)

NIST is proposing the development of the Open Security Controls Assessment Language, or OSCAL, a hierarchical, formatted, XML-based (and JSON translation) schema that provides a standard for representing different categories of information pertaining to the publication, implementation, and assessment of security controls.

OSCAL is attempting to address a number of challenges around security controls and security controls assessment. The core challenge, and one of the primary reasons for creating OSCAL, is that concepts like security controls and profiles are represented today largely in proprietary ways. In many cases they are written in prose documents that are imprecise, lead to differences in interpretation, and are not machine-readable, meaning that the prose instructions require someone to do data entry into a tool in order for the tool to use the information.

Organizations are also struggling with information systems that have many different components, and some components require the use of different profiles per component, which is commonly the case with cloud environments. Also, the cloud environments can be multitenant or have mixed ownership of components. We need to be able to assess the security of these systems against a number of requirements, owners, etc.—to do this simultaneously and provide these views to stakeholders.

In addition, there are situations where a single system needs to support multiple regulatory frameworks. For example, the U.S. Department of Veterans Affairs is a federal agency (with Federal Information Security Modernization Act (FISMA) and NIST Cybersecurity Framework requirements) and a healthcare institution (with Health Insurance Portability and Accountability Act (HIPAA) requirements) that has credit card transactions (with requirements specified in the Payment Card Industry Data Security Standard (PCI DSS)). There is no shortage of requirements for some organizations that have multiple regulatory frameworks. Assessing a plethora of security controls rooted on different standards with different formatting is a complex process that is currently largely manual or leverages proprietary, specifically customized approaches and tools.

OSCAL attempts to standardize how security controls are represented, how a control implementation for a given system is represented, and how that information is best used. It supports the generation of standardized reports that can be used by both humans and machines. That means that formats are needed that can be generated by machines for communicating with other machines, but can also be easily reformatted so that humans can read the information. By standardizing the representation of this information, OSCAL information can be interoperable because of a well-defined specification with information that's going to be used, imported, and subsequently used for security control assessments. The goal is to keep OSCAL as simple as possible and provide extensive automation for tools it uses.

During FY 2017, NIST focused on developing the control catalog schema and the profile schema, focusing on addressing a large number of user stories that describe features, attributes or characteristics. The team validated the approach with use cases from SP 800-53 Rev. 4, SP 800-53 Rev. 5 (draft), ISO/IEC 27001 and 27002, and COBIT 5.

In the next year, NIST will continue the development of the other schemas pertaining to the project (e.g., the framework schema, implementation schema and System Security Plan (SSP) representation, assessment schema, etc.).

CONTACTS:

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

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

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md., is a collaborative hub – convening experts from industry, academia, and government to work on critical problems in cybersecurity. The NCCoE's collaborations focus on providing practical guidance to technical, real-world cybersecurity challenges using standards-based, commercially available technologies.

Project Lifecycle

To help accelerate businesses' adoption of standards-based, secure technologies, the NCCoE works collaboratively with stakeholders to:

- **Define and articulate:** The NCCoE works with industry stakeholders, cybersecurity professionals, academic experts, government agencies, and others to identify and define pressing cybersecurity issues.
- **Organize and engage:** The NCCoE then collaborates with stakeholders to refine a project's scope and develop detailed technical descriptions of the problem. The NCCoE also engages technology vendors via an open call through the Federal Register, to build a potential example solution.
- **Implement and test:** The NCCoE works with technology vendors that have standards-based, commercially available products that can be used as part of the example implementation. These vendors sign a Cooperative Research and Development Agreement (CRADA) and help build a reference design, identify gaps in the build; and refine the example implementation until there is a practical, usable, repeatable reference design that addresses the business problem.
- **Publish and transfer:** The NCCoE provides details of the reference design, standards mapping, lab implementation, and more in a NIST SP 1800 series, a three-volume document that provides applicable guidance for executives, CISOs or IT directors, and IT staff.

Types of Collaborators & Partnerships

Vendors, industry stakeholders, academic experts and others participate in the center through a variety of collaborative mechanisms as described below:

- **Communities of Interest:** A Community of Interest (COI) is a group of professionals and advisors that share business insights, technical expertise, challenges, and perspectives to guide NCCoE projects. The NCCoE relies on this robust collaboration with experts and innovators to provide real-world cybersecurity challenges and inform the reference designs for standards-based cybersecurity integrations that address business needs.
- **Technology Collaborators:** Vendors who would like to participate in a center project reply to a Federal Register call for participation. Vendors who are chosen to participate sign a CRADA and contribute their expertise, hardware, or software to the reference design for a specific problem.
- **National Cybersecurity Excellence Partnership (NCEP):** The NCCoE also works with technology vendors via the NCEP program, wherein vendors sign MOUs to establish a deeper partnership with the NCCoE. NCEPs can provide hardware, software, knowledge, personnel, and can designate guest researchers to work at the center in person or remotely. The NCCoE currently has 31 NCEPs, from Fortune 50 market leaders to smaller companies specializing in IT security.

For more information on NCCoE Partnerships, see https://nccoe.nist.gov/partners.

SP 1800 Series: Practical Cybersecurity Guidance

NCCoE projects result in a NIST Special Publication (SP) 1800 document – a three-volume practice guide, which is a complement to NIST's SP 800 series

documents. SP 1800 documents contain an Executive Summary for business executives, a second volume for security program managers that details security approaches and maps security capabilities to the NIST Cybersecurity Framework as well as other relevant standards, and a third volume for the cybersecurity implementation staff that details the steps needed for another entity to recreate the NCCoE's example solution.

In FY 2017, the center published seven practice guides (up from two in FY 2016 and three in FY 2015) that provide practical guidance, including a reference design and implementation details, on standards-based secure technologies:

1. SP 1800-3, Revision 2, *Attribute Based Access Control;*
2. SP 1800-6, *DNS-Based Email Security;*
3. SP 1800-7, *Situational Awareness for the Electric Utilities;*
4. SP 1800-8, *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations;*
5. SP 1800-9, *Managing Access Rights in the Financial Services Sector;*
6. SP 1800-11, *Data Integrity: Recovering from Ransomware and Other Destructive Events;* and
7. SP 1800-12, *Derived Personal Identity Verification (PIV) Credentials.*

For more information about NCCoE projects, visit https://nccoe.nist.gov/projects.

Example: Impact of Guidance on Wireless Infusion Pumps

Medical devices like infusion pumps were once standalone instruments. Today, infusion pumps connect wirelessly to a variety of healthcare systems, networks, and other devices. Connecting infusion pumps to point-of-care medication systems and electronic health records can improve healthcare delivery processes, but it also increases cybersecurity risks that could affect operations or safety. Tampering with the wireless infusion pump ecosystem, whether intentionally or otherwise, can expose a healthcare delivery organization to serious risks, including breaches of protected health information, loss or disruption of healthcare services, damage to an organization's reputation, productivity, and revenue, or even loss of life.

The NCCoE worked with a community-of-interest made up of various components of the healthcare ecosystem to define the challenge of using wireless infusion pumps securely, identify relevant standards and best practices, and create a representative architecture.

The NCCoE then developed a lab implementation to demonstrate how healthcare delivery organizations can use standards-based, commercially available cybersecurity technologies and industry best practices. Working with five major infusion pump manufacturers, which accounted for 85 % of the market in America, and innovative cybersecurity technology vendors, the NCCoE helped highlight where security capabilities could be built into the pumps to strengthen the cybersecurity of the devices, pump ecosystem, and healthcare enterprise. This has led to multiple pump manufacturers incorporating security capabilities into the next generation versions of their pumps.

Collaborating Across Government

The NCCoE's Work for Others (WFO) Program, governed by the NCCoE's Program Management Office (PMO), facilitates the engagement of other agencies with NIST's National Cybersecurity Federally Funded Research and Development Center (FFRDC). Since 2015, the WFO program has continuously grown and currently has several interagency agreements in place, which support projects for the U.S. Coast Guard, the U.S. Department of Transportation, the U.S. Air Force, and the Department of Homeland Security.

Example of Government Collaboration: U.S. Coast Guard and Sector CSF Profiles

In early FY 2017, the U.S. Coast Guard (USCG) and industry representatives worked with NIST to develop the Maritime Bulk Liquids Transfer Cybersecurity Framework (CSF) Profile. This profile template helps organizations in the complex and sophisticated supply chain of the oil and natural gas industry assess and monitor their cybersecurity risk (see https://www.dco.

uscg.mil/Portals/9/CG-FAC/Documents/Maritime_BLT_CSF.pdf?ver=2017-07-19-070544-223). Building on the success of this CSF profile, the USCG asked for two more profiles to be completed: Mobile Off-Shore Drilling Units and Passenger Vessels.

The goal of these profiles is to provide maritime sub-sectors with guidance for applying the CSF, leveraging the framework to create a sub-sector profile that individual companies can tailor and use to prioritize resources and identify cybersecurity gaps. This project has helped showcase how the NCCoE can apply standards and best practices to real-world industry challenges to help companies more easily take advantage of existing guidance.

Workshops & Events

Figure 36: The Enhancing Resilience of the Internet and Communications Ecosystem Workshop

Throughout FY 2017, the NCCoE hosted and participated in numerous workshops to define, refine, and provide guidance on technical cybersecurity challenges facing businesses today.

For example, the NCCoE hosted NIST's Workshop on "Enhancing Resilience of the Internet and Communications Ecosystem," which brought together over a hundred cybersecurity technologists, vendors, researchers, and subject matter experts. Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," required the Secretaries of Commerce and Homeland Security to "jointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the internet and communications ecosystem and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)." The workshop was designed to allow stakeholders to explore a range of current and emerging solutions addressing automated, distributed threats in an open and transparent manner. The workshop's proceedings were detailed in NISTIR 8192, published in FY 2017 (see https://csrc.nist.gov/publications/detail/nistir/8192/final). Beyond NISTIR 8192, the workshop led to the launch of two new NCCoE projects: *Mitigating IoT Based Automated Distributed Threats* and *TLS Server Certificate Management*.

Additionally, the regularly held NCCoE Speaker Series showcases thought leaders that highlight critical cybersecurity issues of national importance across various industries. The Speaker Series is jointly hosted by the NCCoE, Maryland Department of Commerce, and Montgomery County Department of Economic Development in collaboration with the Maryland Tech Council. This year, the NCCoE hosted four Speaker Series events, whose topics ranged from how small businesses can utilize the NIST CSF, to cybersecurity threats in the hospitality sector, to the psychology behind insider threats.

The NCCoE also hosted multiple in-person workshops with its NCEP partners – in February at the RSA Conference and in September at Juniper Networks' headquarters in Sunnyvale, CA. The workshops brought together dozens of top cybersecurity experts from nearly all the partner organizations to discuss critical cybersecurity challenges, from identity to artificial intelligence, that may benefit from NCCoE guidance.

Learn more about the NCCoE's events at https://nccoe.nist.gov/events.

Looking Ahead

Building on the robust stakeholder engagement seen in FY 2017, the NCCoE expects to accelerate the number of projects undertaken in FY 2018, reinforcing the importance of the Healthcare, Financial Services, and Energy industries as well as expanding work in identity and access management, the Internet of Things, and Internet infrastructure.

FOR MORE INFORMATION SEE:

https://nccoe.nist.gov

CONTACTS:

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

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

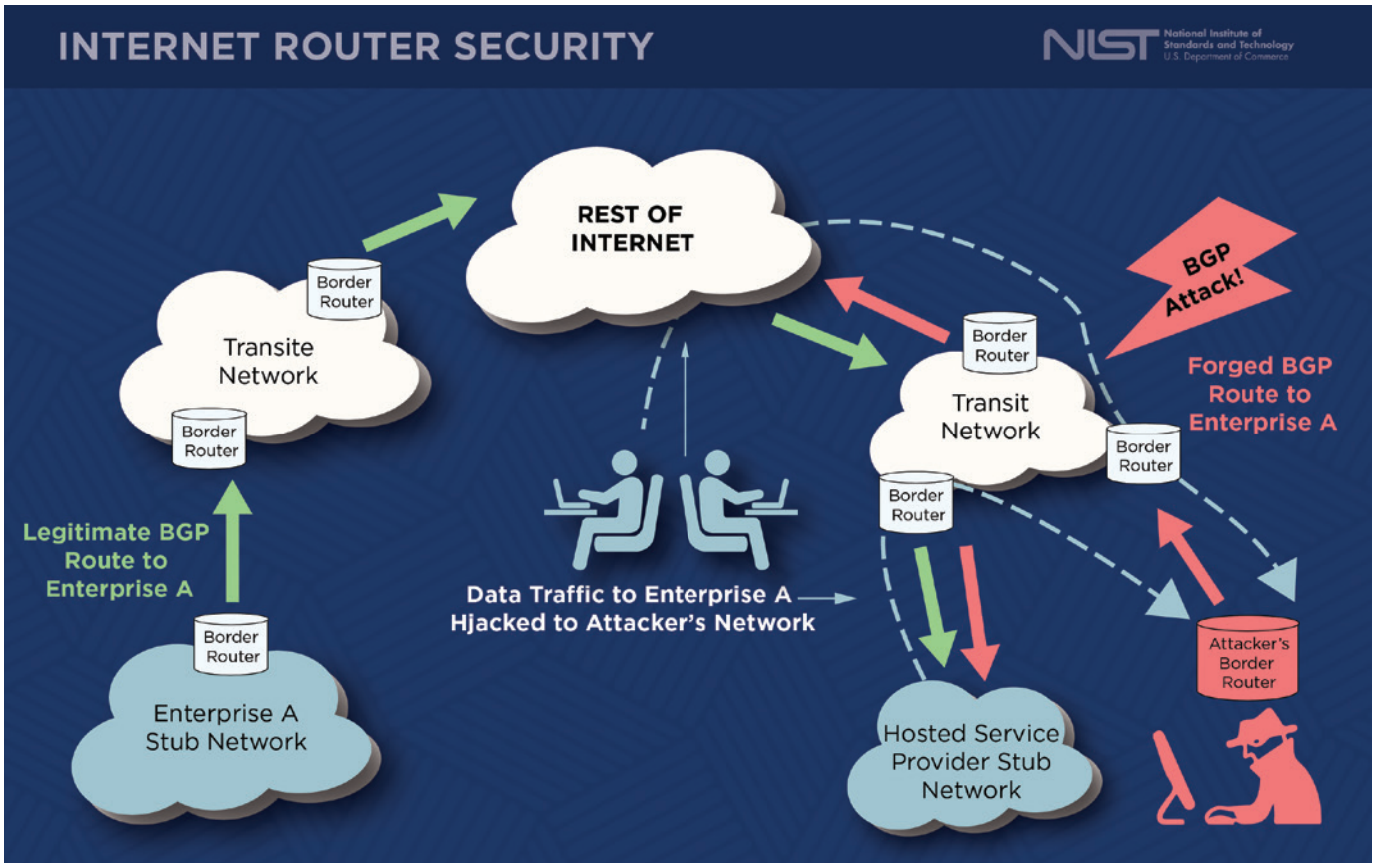
Mr. Tim McBride
(301) 975-0214
timothy.mcbride@nist.gov

Ms. KarenWaltermire
(301) 975-0221
karen.waltermire@nist.gov

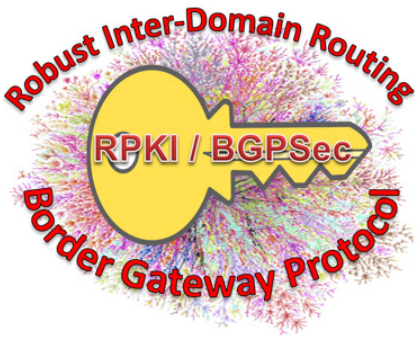
INTERNET INFRASTRUCTURE PROTECTION

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 resilience and security of the global Internet. The research focuses on the development of measurement and modeling techniques necessary to understand, predict, and control the behavior of Internet-scale networked information systems. The ITL staff use these techniques 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 several of the foundational routing and communications protocols - the Internet's Domain Name System (DNS), 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.

The ***Robust Inter-Domain Routing (RIDR)*** project aims to remedy serious security and robustness vulnerabilities in the Internet's global BGP routing system. In FY 2017, the ITL staff, working with its Internet Engineering Task Force (IETF) partners, completed the design and standardization of the *BGPsec Protocol Specification (RFC8205)* and



supporting specifications. BGPsec provides the ability to use digital signatures to prevent both malicious and accidental unauthorized routing messages from effecting Internet global routing operations.



In addition to standards development, NIST developed and released an open source reference implementation of emerging IETF BGPsec specifications, on-line test tools to foster their adoption and measurement systems to track their operational deployment. Figure 37 is a visualization generated by one such monitoring tool that shows the current state of Route Origin Authorizations (ROAs) in the global Resource Public Key Infrastructure (RPKI). The RPKI has been designed to provide the trust infrastructure upon which Internet routing security technologies can be based.

In FY 2017, as BGPsec and RPKI technology specifications and implementations matured, ITL shifted its efforts to focus on technology transition and operational issues associated with the new secure routing technologies. The ITL staff and its collaborators published research results on high-speed BGPsec implementations that attempt to minimize the operational performance impact of routing security. Figure 38 illustrates a prototype model for investigating and validating the emerging BGP security extensions and supporting protocols.

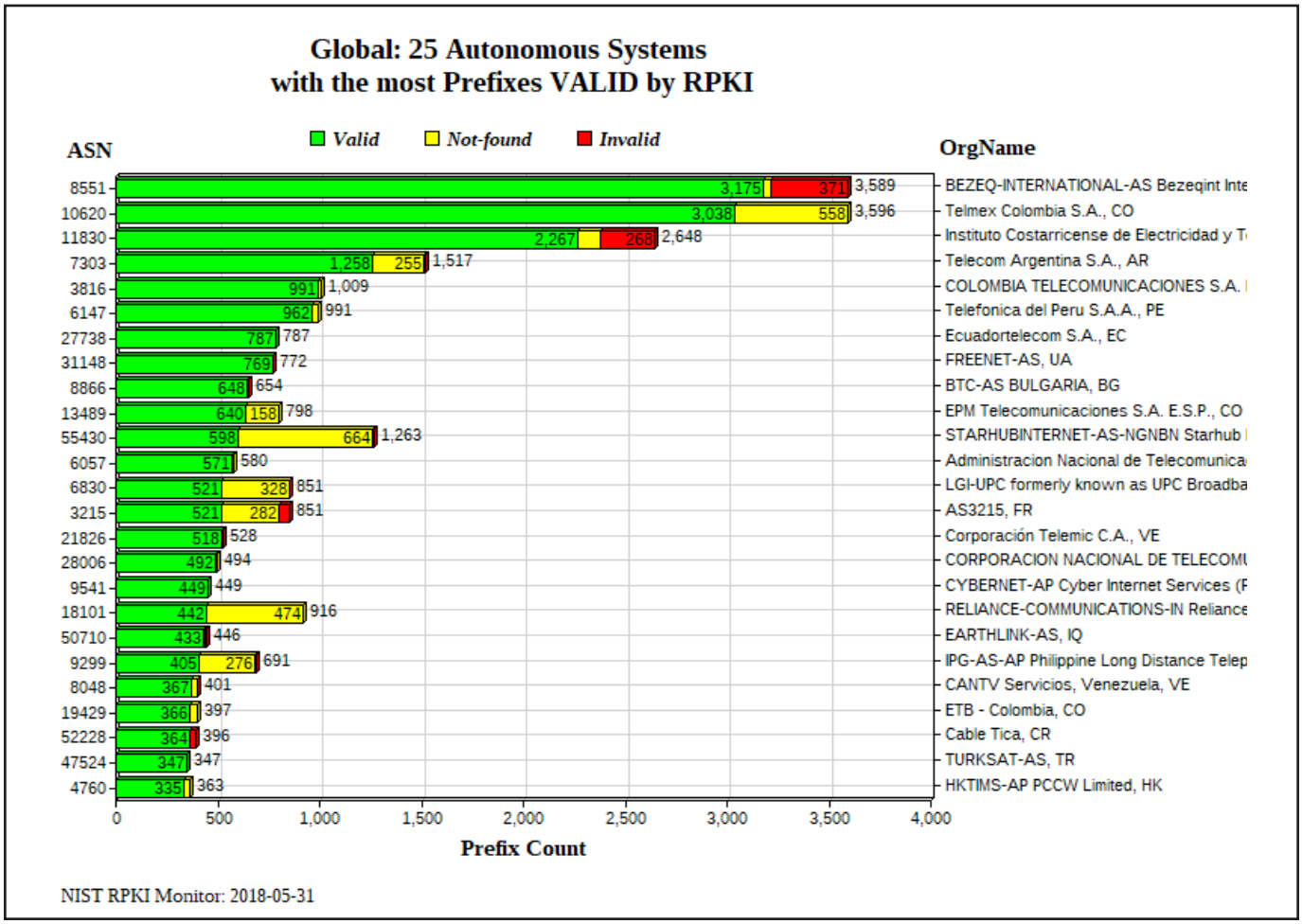


Figure 37: Measurement of global networks with most BGP announcements protected by RPKI.

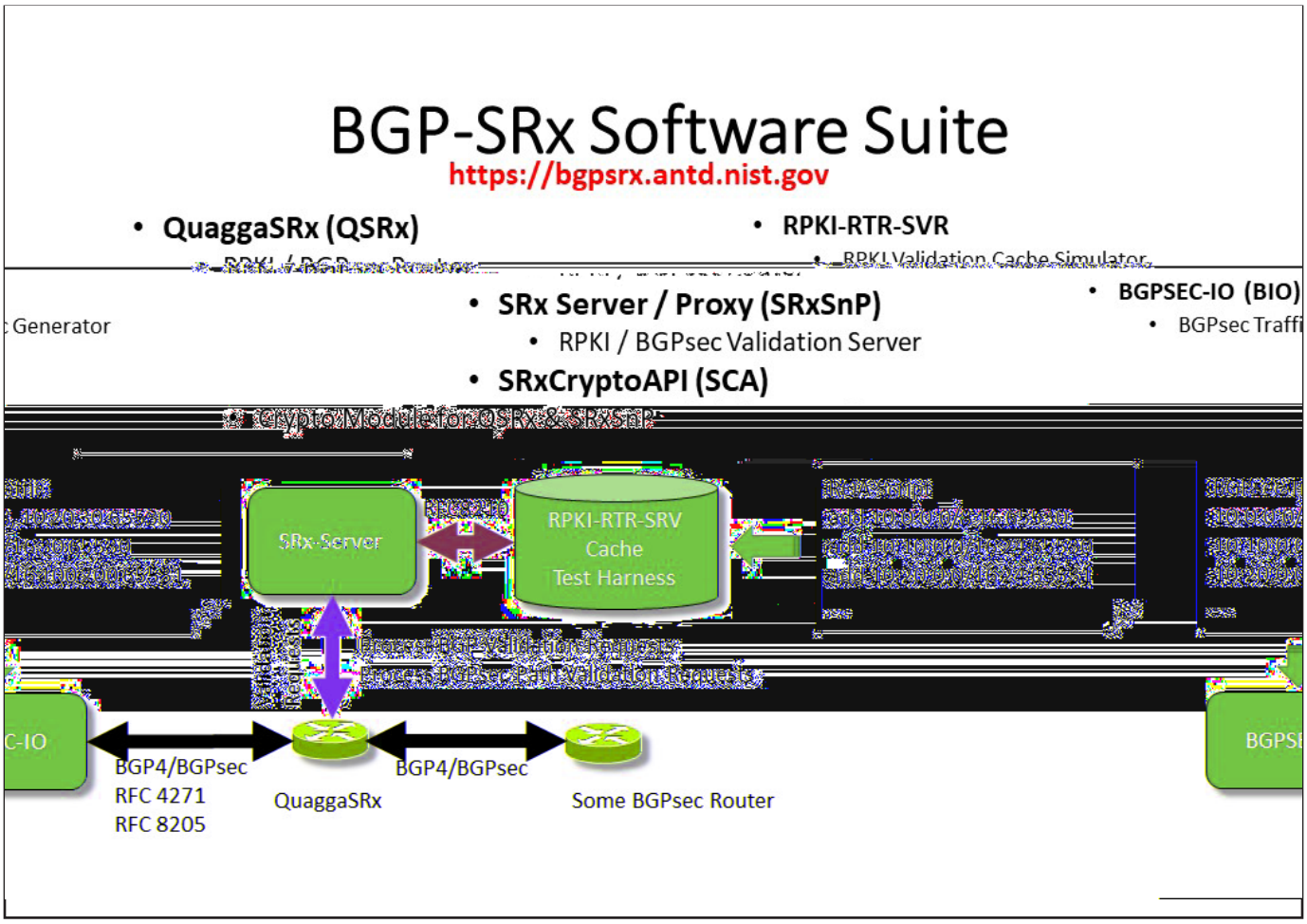


Figure 38: NIST BGPsec prototypes and test tools

To further facilitate technology transition, a new *NCCoE Secure Inter-Domain Routing (SIDR)* project was initiated with industry partners to conduct a proof-of-concept evaluation of the current state of secure routing technologies in realistic deployment settings.

A second thrust of ITL's RIDR project is addressing the wide-spread problem of BGP "route leaks" – accidental routing policy violations that often result in large-scale outages in global Internet routing. The ITL staff have lead the development of IETF specifications that define the problem space (see RFC 7809, *Problem Definition and Classification of BGP Route Leaks*) and the corresponding proposed mitigation techniques.

FOR MORE INFORMATION:

NIST RPKI monitor
https://rpki-monitor.antd.nist.gov/

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

NCCoE Secure-Inter-Domain Routing Project
https://nccoe.nist.gov/projects/building-blocks/secure-inter-domain-routing

CONTACTS:

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

Dr. Kotikalapudi Sriram
(301) 975-3973
ksriram@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 2017, CSD has continued 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, the 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 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 by releasing additional drafts in FY 2018 to ensure participation from as many stakeholders in the vulnerability community 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.

Credit: Shutterstock/Den Rise

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 3 for details.

Since the release of SCAP 1.2, CSD has worked to improve guidance for using 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, NISTIR 8058 documents best practices for content creation and encourages their use by SCAP content authors and maintainers. Feedback on this document is welcomed and will help CSD to work toward producing a final version of this NISTIR 8058.

Credit: Shutterstock/Titima Ongkantong

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.

CSD is currently working to publish the final versions of the publications described above in early FY 2018. CSD has published a beta release of an updated version of SCAPVal, the SCAP content validation tool. A final version of this tool will be provided after the SP 800-126 documents have been finalized. CSD is also working to update the SCAP Validation Program to support SCAP 1.3, with an update to NISTIR 5711 to be posted in early FY 2018. More information on SCAP 1.3 can be found at: https://csrc.nist.gov/Projects/Security-Content-Automation-Protocol/SCAP-Releases/SCAP-1-3.

CSD is also starting to plan an SCAP 2.0 release (SCAP v2). 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 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 for orchestrating courses of action. CSD is preparing a draft whitepaper for release in early FY 2018 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. A discussion draft of the SCAP 2.0 specification addressing software asset management and vulnerability management use cases will also be published in FY 2018 as a way to start a broader conversation with the SCAP community about where to focus next on the development of SCAP 2.0.

TABLE 3: 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) 5.11.2	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

Software Asset Management Standards

CSD has been collaborating with industry partners to promote the adoption of ISO/IEC 19770-2:2015, *Information technology—Software asset management—Part 2: Software identification tag*, which establishes a specification for tagging software to support identification and management. 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 patching), 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 39 illustrates several types of SWID tags (as indicated in the legend) and how these support multiple elements of the software product life cycle, including deployment, installation, patching, upgrading and removal.

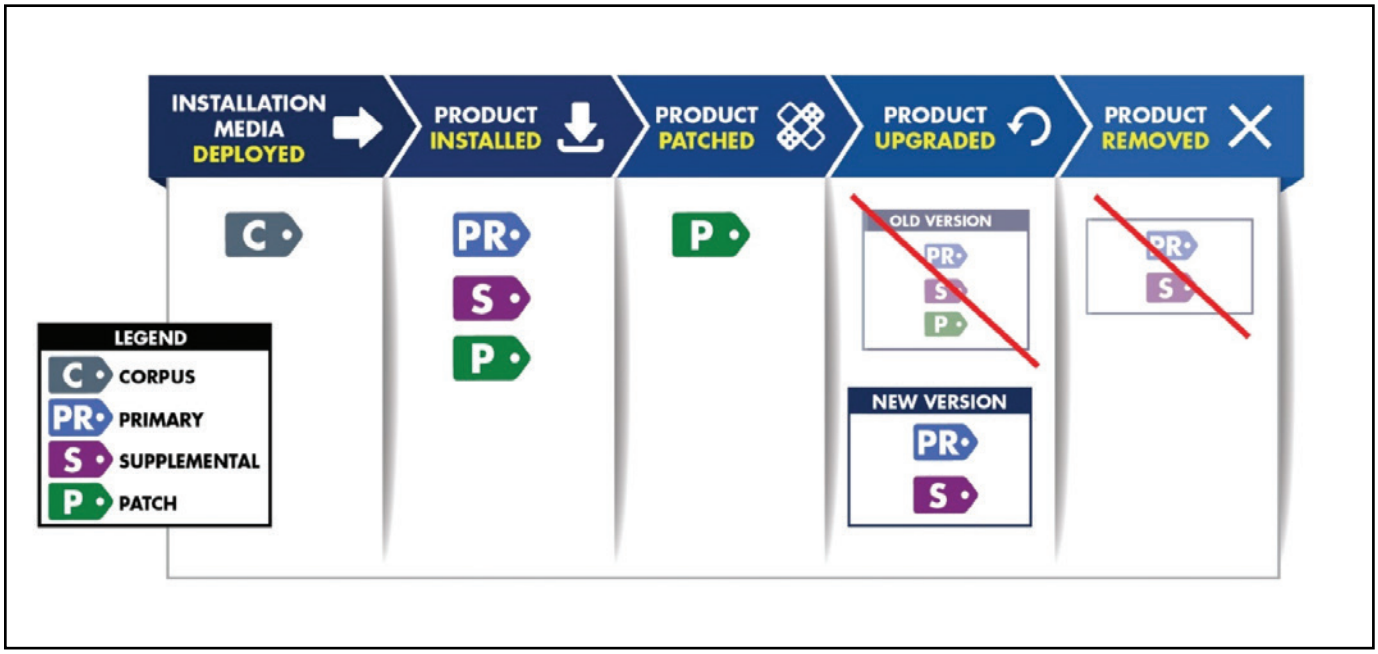


Figure 39: SWID Tags Support the Software Product Lifecycle

Additionally, in FY 2017, NIST has worked with the IETF to integrate SWID tags into the Network Endpoint Assessment (NEA) protocol, through the *Software Inventory Message and Attributes (SWIMA) for PA-TNC* specification (see https://datatracker.ietf.org/doc/draft-ietf-sacm-nea-swima-patnc/). This draft Request for Comments (RFC) will be published soon, describing a method for the automated, event-based collection of software inventory information using SWID tag information.

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. In FY 2017, CSD published a SWID tag validation tool (see https://scap.nist.gov/specifications/swid/), called SWIDVal, that can validate a SWID tag document against the ISO/IEC 19770-2:2015 and NISTIR 8060 requirements.

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 details regarding a device's 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 Trusted Network Connect (TNC) protocol.

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 Trusted Network Connect (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. IF-M is a messaging protocol that helps communicate measurement information about endpoints for evaluation against security policy. The second is the TNC Endpoint Compliance Profile (ECP) and related specifications that support the exchange of SWID data over the TNC protocols. The ECP enables the collection of SWID data from a device for use by external tools to provide software inventory information. SCAP and SWID data collected using these mechanisms may be optionally used for network access control decision making, allowing the device state to be evaluated when devices connect and on an ongoing basis thereafter.

For more information on this specification, please visit: 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 and MILE working groups, which are available through the locations indicated in Table 4.

The SACM and MILE working groups have been developing the following related Internet Drafts:

INTERNET DRAFT	PURPOSE
https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid/	A Concise Binary Object Representation (CBOR) [RFC7049] based specification for representing SWID tag for use with constrained IoT devices.
https://datatracker.ietf.org/doc/draft-ietf-sacm-ecp/	Specifies the Endpoint Compliance Profile (ECP), that describes the use of IETF and TNC protocols and interfaces to support the ongoing assessment of endpoint posture and the controlled exposure of collected posture information to authorized security applications.
https://datatracker.ietf.org/doc/draft-ietf-sacm-nea-swima-patnc/	Extends the PA-TNC specification [RFC5792] to provide specific attributes and message exchanges allowing endpoints to report their installed software inventory information to a NEA server.
https://datatracker.ietf.org/doc/draft-ietf-mile-rolie/	The ROLIE protocol supporting a resource-oriented approach for security automation information publication, discovery, and sharing.
https://datatracker.ietf.org/doc/draft-ietf-sacm-rolie-softwaredescriptor/	An extension to ROLIE to support the exchange of SWID-based software information.
https://datatracker.ietf.org/doc/draft-ietf-sacm-terminology/	Definition of the common terminology used within several working-group documents.

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 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:

https://scap.nist.gov/

CONTACT:

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

Security Automation Reference Data

Through the National Vulnerability Database and the National Checklist Program (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 2017, the NVD contained the following resources:

- Over 96,000 vulnerability advisories, with an average of 62 new vulnerabilities added daily;
- 183 SCAP-expressed checklists across 123 platforms 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; 4,467 US-CERT vulnerability summaries; and 10,286 SCAP machine-readable software flaw checks; and
- A product dictionary with over 124,000 operating system, application, and hardware name entries; and over 75,000 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.

In the past year, the NVD began providing CVSS base scores following the CVSS v3 specification within the data feeds and completed a major enhancement to the overall user interface. The NVD has also seen a significant increase (almost three fold) in vulnerabilities received and analyzed over the previous year. Overall, the NVD has experienced an average download growth rate of over 10 % per month.

FOR MORE INFORMATION, SEE:

https://nvd.nist.gov

CONTACT:

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.

Credit: Shutterstock/Natali_ Mis

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 the use of common security configurations available from the NIST website at https://checklists.nist.gov. Agency contracting officers should consult with the requiring official to ensure that 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.

At the end of FY 2017, there are a total of 476 checklists posted on the NCP website (see https://checklists.nist.gov/). Of that total, 183 of the checklists, addressing 123 platforms, are SCAP-expressed and can be used with SCAP-validated products.

Organizations can use the 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/).

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 https://csrc.nist.gov/publications/PubsSPs.html.

In 2017, NIST released a draft version of SP 800-70 Revision 4, which can be viewed at https://csrc.nist.gov/CSRC/media/Publications/sp/800-70/rev-4/draft/documents/sp800-70r4-draft.pdf. SP 800-70 Revision 4 will be published as final in FY 2018, and the checklists.nist.gov website will be modified to reflect the updated document.

FOR MORE INFORMATION, SEE:

https://checklists.nist.gov

CONTACT:

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

Apple macOS Security Configuration

CSD's macOS security configuration team is working to develop secure system configuration baselines supporting different operational environments for Apple macOS version 10.12, "Sierra." These configuration guidelines will assist organizations with hardening macOS technologies and provide a basis for unified controls and settings for federal macOS workstation and mobile system security configurations. The configurations are based on a collection of resources, including the existing NIST macOS configuration guidance, the Defense Information Systems Agency (DISA) macOS Security Technical Implementation Guide (STIG), and the Center for Internet Security (CIS) macOS Security Benchmark.

The project team researched and tested approximately 270 settings for macOS 10.12. The configuration set has been significantly reduced due to changes in the operating system's features and default setting values. Among other collected data, each setting has a designated Common Configuration Enumeration (CCE) number, which aids in its long-term tracking. Figure 40 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.

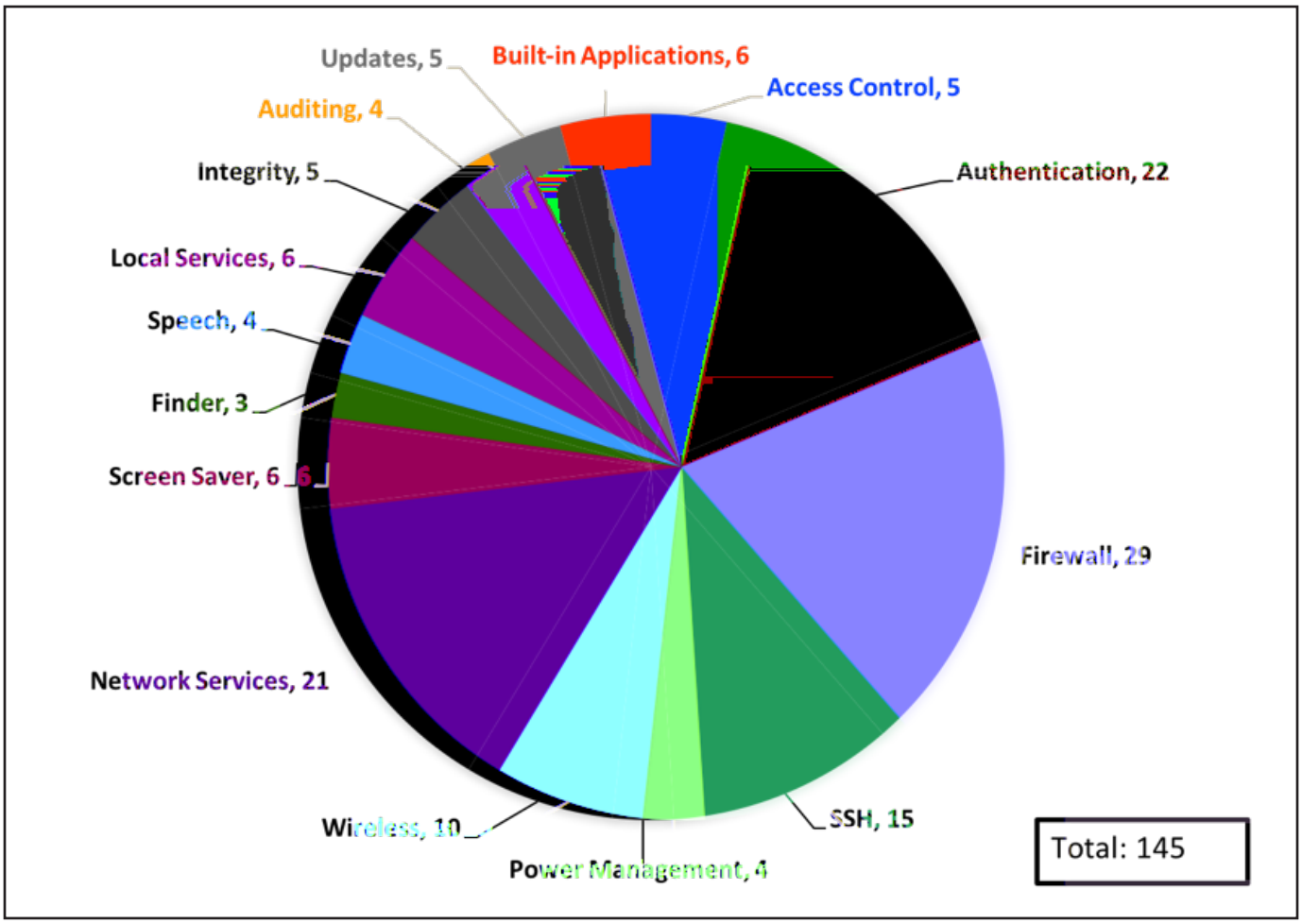


Figure 40: Configuration Categories

The shell scripts that apply the settings to a macOS 10.12 system 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 2017, the final version of SP 800-179, *Guide to Securing Apple OS X 10.10 Systems for IT Professionals* was published. This document explains the settings, their security significance, and how to configure them for the three baselines described above. The project team then focused on updating the guide, script and spreadsheet of settings for Apple macOS 10.12 systems.

In FY 2018, the team plans to:

- Produce an updated guide for macOS 10.12;
- Continue to refine the script and add more settings to the configuration; and
- Investigate macOS 10.13, "High Sierra."

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/projects/apple-os-x-security-configuration
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

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. Considered as an emerging branch of forensics that combine network and systems forensics, cloud forensics addresses post-incident analysis of systems with the complexities of distributed processing, multi-tenancy and virtualization. CSD has developed a framework that shows what evidence can be used to reconstruct corresponding attack scenarios in the cloud, and discusses how this framework can be applied to automate the forensics analysis in the cloud with the objective of saving a forensics investigator's time.

CSD has also developed a layered graphical model to analyze the impact of cyber attacks on business processes and services. The model has three layers: the upper layer models that the business processes and their dependencies, the middle layer constructs attack scenarios using evidences in log files, and the lowest layer reconstructs the missing attack steps using system calls. Based on the graph produced from the three layers, the model computes a quantitative impact on the business processes. CSD has developed a case study that shows the usability of this model and how it can be applied for both forensics analysis and for mitigating the impact of cyber attacks on the enterprise infrastructure. CSD published two papers in this area:

1. Identifying Evidence for Cloud Forensics Analysis, International Federation for Information Processing (IFIP) International Conference on Digital Forensics, Orlando, FL, January 29 - February 1, 2017.

2. Towards Actionable Mission Impact Assessment in the Context of Cloud Computing, 31st IFIP WG 11.3 Conference on Data and Application Security and Privacy, Philadelphia, July 19-21, 2017.

In FY 2018, CSD plans to develop new techniques and metrics for Cloud Computing forensics analysis and mission impact analysis. CSD also plans to publish the results as a NIST report and as white papers in conferences and journals.

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/projects/measuring-security-risk-in-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.

In FY 2017, the AIM project completed research in several areas: it proved that an important access control system is scalable, created novel metrics for defense-in-depth measurement, and identified an important intrusion detection approach. More specifically, the project team accomplished the following:

- The team proved that the NGAC model is scalable by providing a fast-linear time, decision algorithm when existing reference implementations used slow cubic algorithms. This enables enterprises to reduce insider threats by tightly controlling data access through simultaneous instantiation of multiple access control policies (the research was published in the *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* and the *Proceedings of the 2016 International Workshop on Managing Insider Security Threats*).
- The team created novel metrics to measure the defense-in-depth posture of network systems. They proved that the metrics are extremely difficult to calculate (NP-Hard), and thus provided efficient and accurate approximation algorithms (this research was published in the proceedings of the *Proceedings of the 2nd Annual Industrial Control System Security Workshop*).
- The team discovered that *n*-gram anomaly detection (the most successful anomaly detection method to date) can act primarily as a signature system. This happens, in a form we call micro-signatures, when removing attacks from within test data in order to train on a clean set of data. This result reveals a new methodology for hybrid anomaly/signature detection systems while also calling into question many past anomaly detection results (this research was published in the proceedings of the *International Symposium on Foundations and Practice of Security*).

In FY 2018, the AIM project will work on evaluating the privacy of global Internet traffic, architectures for cryptocurrencies to limit criminal behavior, secure methods for transactions involving digital goods, and how to publish trustworthy random numbers using blockchains and smart contracts.

FOR MORE INFORMATION, SEE:

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

CONTACT:

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

Automated Combinatorial Testing

Software engineers often encounter failures that result from an unexpected interaction between components. A 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 41); 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 practical 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 2017 include the development of a mathematical model that closely replicates the evolution and distribution of t-way failures found in empirical studies; invited lectures at conferences and universities; leading the Sixth International Workshop on Combinatorial Testing, held in conjunction with the Ninth IEEE International Conference on Software Testing; the development of combinatorial test methods specific to text search, with a demonstration of their practical application; and the development of combinatorial test methods specific to cryptographic software that discovered previously unknown faults in AES algorithm implementations. Collaborators include researchers from the University of Texas at Arlington, the University of Texas at Dallas, Loyola University of Maryland, East Carolina University, Duke University, Texas A&M, and the Air Force Institute of Technology.

Technology transfer activities included the publication of a number of technical papers and software distributions; input to DoD recommendations on software test and verification; the release of enhanced combinatorial measurement tools; input modeling and fault location tools; the development of new test methods and tools specific to cryptography; the development of new test methods and tools specific to full-text search; and seminars at conferences, universities, and federal agencies.

Plans for FY 2018 include the development of methods and tools for testing cyber-physical systems and IoT systems; a potential application to place smart contract functions on a blockchain; methods for reducing the generation cost of high-assurance and life-critical software requirements; a trial use of prototype methods and tools for oracle-free testing methods; the 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.

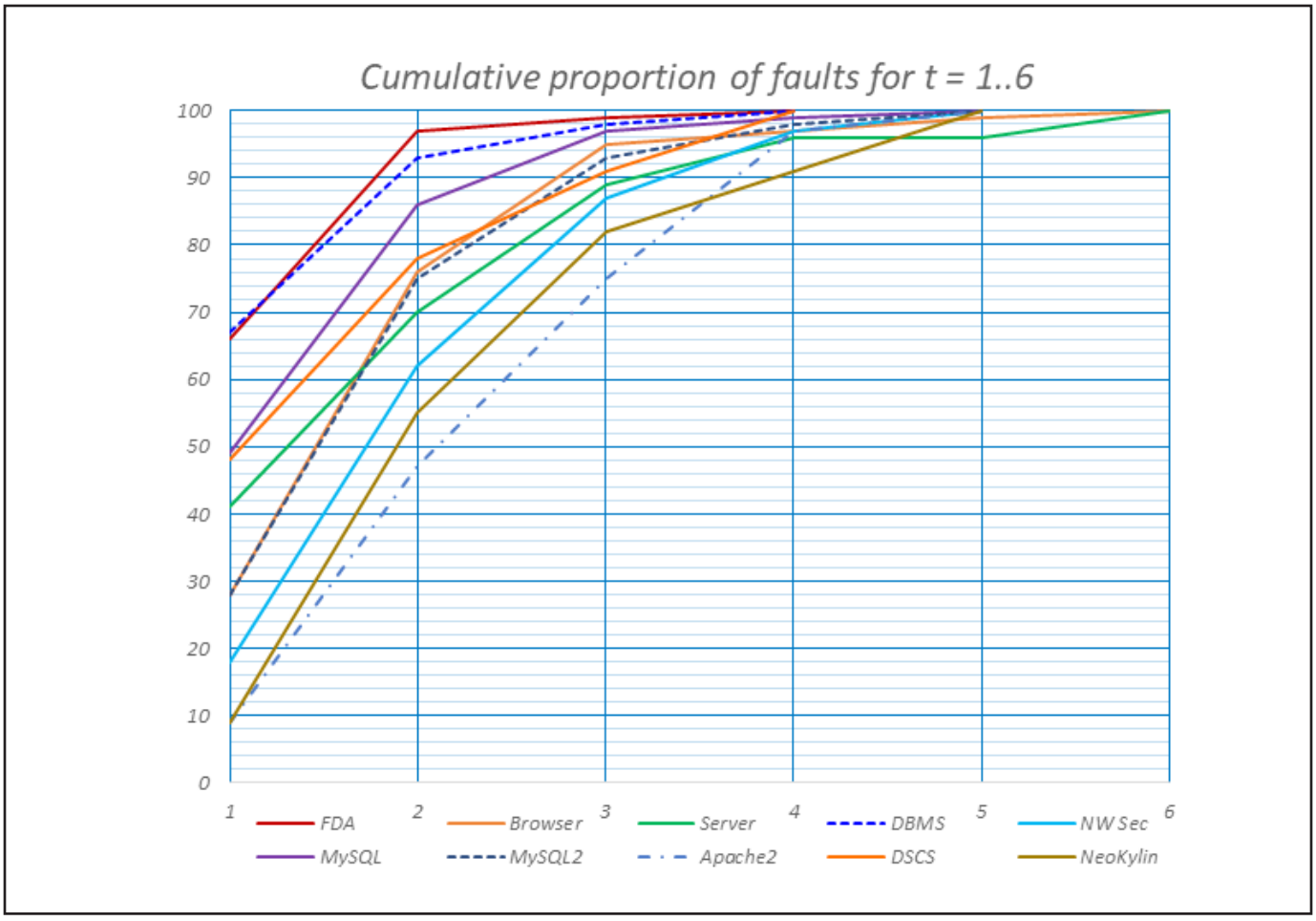


Figure 41: Distribution of failures at t = 1..6

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/projects/automated-combinatorial-testing-for-software

CONTACTS:

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

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

Roots of Trust

Modern computing devices consist of various hardware, firmware, and software components at multiple layers of abstraction (see Figure 42). 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.

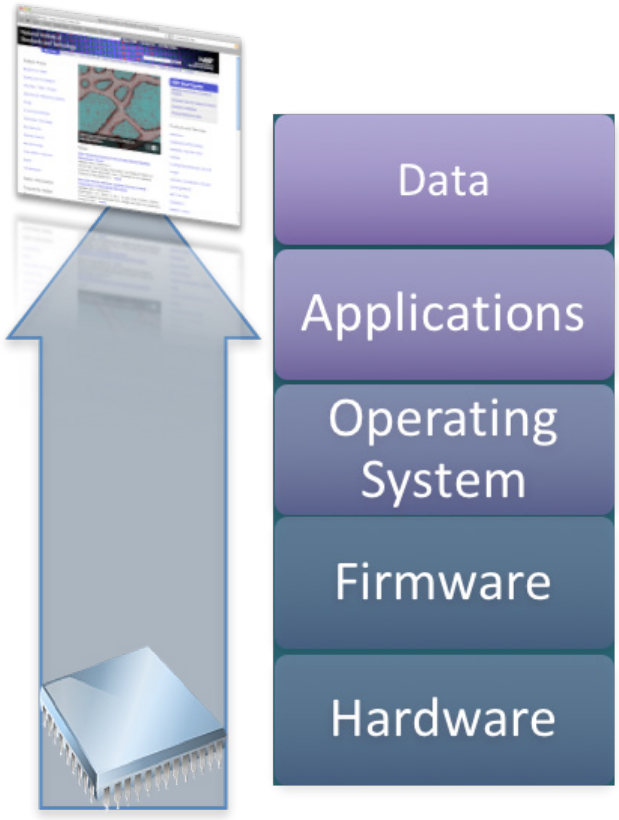


Figure 42: Layers of Abstraction within a Mobile Computing Device

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 as part of the 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*.

A new effort in FY 2017 built upon that earlier work focused on boot firmware to research and develop techniques and guidelines for securing firmware throughout the platform. Released for public comment in May 2017, SP 800-193, *Platform Resiliency Guidelines*, provides technical guidelines and recommendations supporting the resiliency of platform firmware and data against potentially destructive attacks. These draft guidelines promote resiliency in the platform by describing security mechanisms for protecting the platform against unauthorized changes, detecting unauthorized changes that occur, and secure recovery from attacks.

These new draft guidelines have been the basis for discussions with industry, standards organizations, and consortiums over technologies, standards, and specifications that can improve the resiliency of computer platforms using roots of trust. Based on these discussions, NIST expects to finalize SP 800-193 in FY 2018 and continue outreach to stakeholders in government, industry, and academia to encourage the development of more secure and reliable systems.

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/projects/hardware-roots-of-trust

CONTACT:

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

USABILITY AND SECURITY

The goal of the Usable Security and Privacy team, part of ITL's Information Access Division (IAD), is to provide guidance for policymakers, system engineers and security professionals so that they can make better decisions that enhance the usability of cybersecurity in their organizations.

During FY 2017, the team contributed usability chapters to SP 800-63, *Digital Identity Guidelines*, marking the first time that there were dedicated usability chapters in this publication.

Phishing Awareness Training and Evaluation

During FY 2017, the usability team completed a long-term operational phishing evaluation, demonstrating the importance of individual user context in explaining phishing email click decisions; this collaboration provided the supporting data necessary to interpret the previously puzzling variability in click rates observed across prior years of operational phishing awareness training exercises.

The team performed research regarding attacks known as phishing, where a sender initiates an email containing fraudulent information with the intent of inducing the recipient to reveal sensitive information. Phishing continues to be an escalating cyber threat facing organizations of all types and sizes, including industry, academia, and government. To help combat the phishing threat, many organizations utilize phishing awareness training to make employees and students more aware of phishing threats and consequences. Phishing awareness training systems often use software to emulate real-world threats and thus train people to recognize and avoid falling victim to phishing attacks. Using this type of embedded training system, researchers in the usability group partnered with NIST's OISM (Office of Information Systems Management) and OSHE (Office of Safety Health and Environment) to complete three phishing awareness training exercises with corresponding surveys, culminating a multi-year phishing awareness evaluation.

With the data developed, usability researchers have successfully answered both an operational assessment question, *Why are users clicking or not clicking on phishing links and attachments?*, as well as the larger institution's trial deployment question, *Why are click rates so variable?* In contrast to previous research that was primarily performed in laboratory settings, the present work examines 4.5 years of in situ embedded simulated phishing emails. The results have provided additional insights into the rationale that leads some users to become victims of phishing attacks and malicious software. Given the variety of phishing premises and user contexts, no amount of training will consistently reduce click rates to zero, but the findings helped better understand the user's role in early detection, combined with technological solutions, and determined that awareness training and reporting should be fully supported and even incentivized in the workforce.

FOR MORE INFORMATION, SEE:

https://www.nist.gov/itl

CONTACTS:

Mrs. Mary Theofanos
(301) 975-5889
mary.theofanos@nist.gov

Ms. Kristen Greene
(301) 975-8119
kristen.greene@nist.gov

Ms. Michelle Steves
(301) 975-3537
michelle.steves@nist.gov

Digital Identity Guidelines

SP 800-63, *Digital Identity Guidelines,* was finalized and published in June, 2017. After more than a year of work NIST has released a suite of documents covering digital identity from initial risk assessment to deployment of federated identity solutions. The SP suite has also been reorganized. SP 800-63-3 is the base document associated with SP 800-63A, 800-63B, and 800-63C that covers the various components of a digital identity system.

In 2004, NIST published the initial version of Special Publication (SP) 800-63, *Electronic Authentication Guideline*. Since then, two revisions have been published, SP 800-63-2 being published in August 2013. In late 2015, NIST started considering a significant update to SP 800-63-2 in response to

market innovation, evolving federal requirements, and an advanced threat landscape targeting remote authentication. As the first step in revising the publication, NIST solicited recommendations from experts (including those in industry, government, and educational fields) on which sections of the document needed revision. Usability surfaced in many comments as always latent in many security considerations. The usability team was invited to participate in and contribute to this year-long major revision effort. The team participated in weekly meetings with the project team, performed literature reviews, compiled results from our own usable security research, and wrote usability chapters in each of the suite of documents in the new SP 800-63.

Specifically, for SP 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing*, the usability chapter was written to raise implementers' awareness of usability considerations associated with enrollment and identity proofing. For SP 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*, the usability chapter provides usability considerations and guidance on authentication, as integrating usability into the development process can lead to authentication solutions that are secure and usable while addressing users' authentication needs and organizations' business goals. For SP 800-63C, *Digital Identity Guidelines: Federation and Assertions*, the usability chapter provides considerations and guidance to understand user perspectives on online identity, trust and benefits, and user mental models and beliefs in order to promote good user experience with federated identity systems.

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/publications/detail/sp/800-63/3/final

CONTACTS:

Mrs. Mary Theofanos
(301) 975-5889
mary.theofanos@nist.gov

Dr. Yee-Yin Choong
(301) 975-3248
yee-yin.choong@nist.gov

Ms. Kristen Greene
(301) 975-8119
kristen.greene@nist.gov

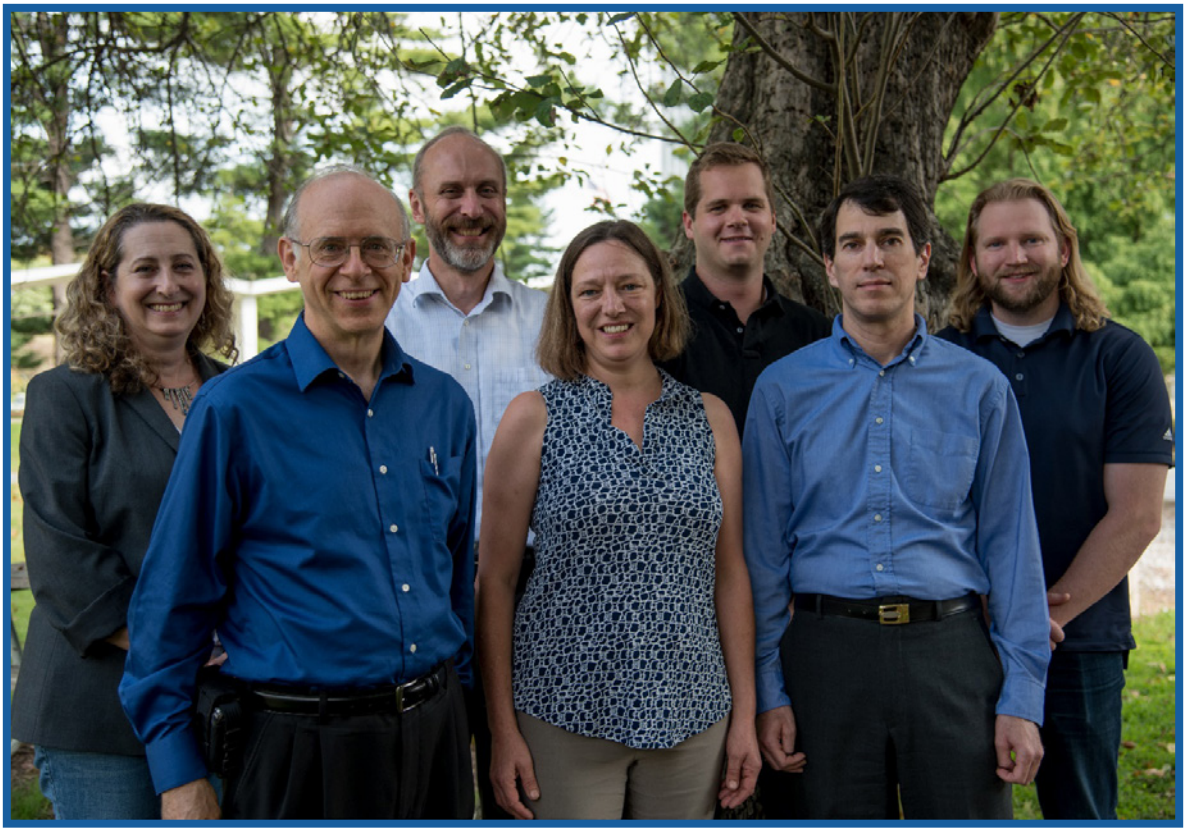
HONORS AND AWARDS

This section recognizes ITL staff who have received honors and/or awards for their cybersecurity accomplishments.

NIST Bronze Medal Award

The Bronze Medal Award is the highest recognition awarded by NIST. The award, approved by the Director, recognizes work that has resulted in more effective and efficient management systems as well as the demonstration of unusual initiative or creative ability in the development and improvement of methods and procedures. It is also given for significant contributions affecting major programs, scientific accomplishments, and superior performance of assigned tasks for at least five consecutive years.

Jeff Cichonski (Applied Cybersecurity Division); Lee Badger, Mike Bartock, David Cooper, Hildegard (Hildy) Ferraiolo, and Murugiah Souppaya (Computer Security Division); Paul Black and Barbara Guttman (Software and Systems Division).



(Left to Right) Back row: B. Guttman, L. Badger, J. Cichonski, M. Bartock
Front row: P. Black, H. Ferraiolo, D. Cooper
Absent: M. Souppaya

The group is recognized for addressing a series of near-term needs and providing a long-term strategy to improve our nation's cybersecurity. The White House-led Cybersecurity National Action Plan of January 2016 prioritized critical cybersecurity areas and directed NIST to produce tools, references, and guidelines to help organizations strengthen the identification and authentication of privileged users, assist in recovering from cybersecurity incidents, self-assess their security capabilities, and identify methods to reduce vulnerabilities in software. The items developed by this team were exceptionally clear, consistent, and actionable, and have led to cybersecurity improvements in all sectors.

Donna Dodson | One of CyberScoop's 2017 Top Women in Cybersecurity

Awarding Organization: CyberScoop

Donna Dodson is the NIST chief cybersecurity advisor. Donna has been named one of CyberScoop's 2017 Top Women in Cybersecurity! Donna Dodson has multiple roles at NIST. In addition to being the chief cybersecurity advisor to Acting NIST Director Kent Rochford, she is associate director of the Information Technology Laboratory — one of six labs at NIST — and director of the National Cybersecurity Center of Excellence.

See NIST Press Release: https://www.nist.gov/about-us/nist-awards/donna-dodson-one-cyberscoops-2017-top-women-cybersecurity

Source:
https://www.cyberscoop.com/top-women-in-cybersecurity-donna-dodson/

Rodney Petersen | 2016 Government Leadership of the Year

Awarding Organization: The Colloquium for Information Systems Security Education (CISSE)

Rodney Petersen is the director of the National Initiative for Cybersecurity Education (NICE) at the National Institute of Standards and Technology (NIST). He previously served as the Managing Director of the EDUCAUSE Washington Office and a Senior Government Relations Officer.

He founded and directed the EDUCAUSE Cybersecurity Initiative and was the lead staff liaison for the Higher Education Information Security Council. Prior to joining EDUCAUSE, he worked at two different times for the University of Maryland - first as Campus Compliance Officer in the Office of the President and later as the Director of IT Policy and Planning in the Office of the Vice President and Chief Information Officer. He also completed one year of federal service as an Instructor in the Academy for Community Service for AmeriCorps' National Civilian Community Corps. He is the co-editor of a book entitled "Computer and Network Security in Higher Education." He received his law degree from Wake Forest University and bachelors degrees in political science and business administration from Alma College. He was awarded a certificate as an Advanced Graduate Specialist in Education Policy, Planning, and Administration from the University of Maryland.

Source:
https://cisse.info/about/award-recipients/634-2016-government-leadership-of-the-year-rodney-petersen

Rodney Petersen and NICE Team - Received the Exemplary International Leadership in Cybersecurity Education and Workforce Development Award

(Left to Right): William (Bill) Newhouse, Marian Merritt. Rodney Petersen, Danielle Santos, Clarence Williams, and Davina Pruitt-Mingle

Awarding Organization: Cyber New Brunswick of Canada

The National Initiative for Cybersecurity Education (NICE) team, which received an award for Exemplary International Leadership in Cybersecurity Education and Workforce Development from Cyber New Brunswick at Canada's inaugural Cybersecurity Education and Workforce Summit (CyberSmart 2017).

Source:
https://www.nist.gov/about-us/nist-awards/rodney-petersen-and-nice-team-received-exemplary-international-leadership

The National Initiative for Cybersecurity Education (NICE) was awarded a recognition plaque at the National Cybersecurity Summit

Awarding Organization: National Cybersecurity Summit

The National Initiative for Cybersecurity Education (NICE) Program Office received an honor of recognition at the National Cybersecurity Summit in Huntsville, Alabama. NICE received this award for its leadership in advancing cybersecurity education, training, and workforce development efforts for the nation.

ITL CYBERSECURITY PROGRAM PUBLICATIONS RELEASED IN FY 2017

This section provides a compilation of ITL cybersecurity publications released during FY 2017 (from October 1, 2016 to September 30, 2017). The first portion lists technical documents, while the second portion provides abstracts that briefly summarize each document (technical and non-technical).

DRAFT PUBLICATIONS

There were no draft FIPS released during FY 2017.

TABLE 5: SPECIAL PUBLICATIONS (SPs)

PUBLICATION NUMBER	TITLE	DRAFT RELEASED
SP 800-193	*Platform Firmware Resiliency Guidelines*	May 2017
SP 800-191	*The NIST Definition of Fog Computing*	August 2017
SP 800-190 (2 Drafts)	*Application Container Security Guide*	April 2017 July 2017
SP 800-188 (2nd Draft)	*De-Identifying Government Datasets*	December 2016
SP 800-187	*Guide to LTE Security*	November 2016
SP 800-177 Rev. 1	*Trustworthy Email*	September 2017
SP 800-125A (2nd Draft)	*Security Recommendations for Hypervisor Deployment*	September 2017
SP 800-70 Rev. 4	*National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*	August 2017
SP 800-67 Rev. 2	*Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*	July 2017
SP 800-56C Rev. 1	*Recommendation for Key Derivation through Extraction-then-Expansion*	August 2017
SP 800-56A Rev. 3	*Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*	August 2017
SP 800-53 Rev. 5	*Security and Privacy Controls for Information Systems and Organizations*	August 2017
SP 800-37 Rev. 2 (Discussion Draft)	*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*	September 2017
SP 1800-12	*Derived Personal Identity Verification (PIV) Credentials*	September 2017
SP 1800-11	*Data Integrity: Recovering from Ransomware and Other Destructive Events*	September 2017
SP 1800-9	*Access Rights Management for the Financial Services Sector*	August 2017
SP 1800-8	*Securing Wireless Infusion Pumps in Healthcare Delivery Organizations*	May 2017
SP 1800-7	*Situational Awareness for Electric Utilities*	February 2017
SP 1800-6	*Domain Name Systems-Based Electronic Mail Security*	November 2016
SP 1800-3 (2nd Draft)	*Attribute Based Access Control*	September 2017

TABLE 6: NIST INTERNAL OR INTERAGENCY REPORTS (NISTIRs)		
PUBLICATION NUMBER	**TITLE**	**DRAFT RELEASED**
NISTIR 8179	*Criticality Analysis Process Model: Prioritizing Systems and Components*	July 2017
NISTIR 8176	*Security Assurance Challenges for Container Deployment*	August 2017
NISTIR 8170	*The Cybersecurity Framework: Implementation Guidance for Federal Agencies*	May 2017
NISTIR 8151	*Dramatically Reducing Software Vulnerabilities: Report to the White House Office of Science and Technology Policy*	October 2016
NISTIR 8139	*Identifying Uniformity with Entropy and Divergence*	February 2017

FINAL APPROVED PUBLICATIONS

There were no FIPS released during FY 2017.

TABLE 7: FINAL SPs		
PUBLICATION NUMBER	**TITLE**	**FINAL RELEASED**
SP 800-195	*2016 NIST/ITL Cybersecurity Program Annual Report*	September 2017
SP 800-192	*Verification and Test Methods for Access Control Policies/ Models*	June 2017
SP 800-190	*Application Container Security Guide*	September 2017
SP 800-185	*SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash*	December 2016
SP 800-184	*Guide for Cybersecurity Event Recovery*	December 2016
SP 800-181	*National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*	August 2017
SP 800-179	*Guide to Securing Apple OS X 10.10 Systems for IT Professionals: A NIST Security Configuration Checklist*	December 2016
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)*	October 2016
SP 800-171 Rev. 1	*Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*	December 2016
SP 800-160	*Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*	November 2016
SP 800-150	*Guide to Cyber Threat Information Sharing*	October 2016
SP 800-121 Rev. 2	*Guide to Bluetooth Security*	May 2017
SP 800-70 Rev. 3 (update)	*National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*	December 2016
SP 800-63-3	*Digital Identity Guidelines*	June 2017
SP 800-63A	*Digital Identity Guidelines: Enrollment and Identity Proofing*	June 2017
SP 800-63B	*Digital Identity Guidelines: Authentication and Lifecycle Management*	June 2017
SP 800-63C	*Digital Identity Guidelines: Federation and Assertions*	June 2017
SP 800-38B (update)	*Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication*	October 2016
SP 800-12 Rev. 1	*An Introduction to Information Security*	June 2017
SP 500-320	*Report of the Workshop on Software Measures and Metrics to Reduce Security Vulnerabilities (SwMM-RSV)*	October 2016

TABLE 8: FINAL NISTIRs		
PUBLICATION NUMBER	**TITLE**	**FINAL RELEASED**
NISTIR 8192	*Enhancing Resilience of the Internet and Communications Ecosystem: a NIST Workshop Proceedings*	September 2017
NISTIR 8183	*Cybersecurity Framework Manufacturing Profile*	August 2017
NISTIR 8165	*Impact of Code Complexity on Software Analysis*	February 2017
NISTIR 8151	*Dramatically Reducing Software Vulnerabilities: Report to the White House Office of Science and Technology Policy*	November 2016
NISTIR 8136	*An Overview of Mobile Application Vetting Services for Public Safety*	January 2017
NISTIR 8114	*Report on Lightweight Cryptography*	March 2017
NISTIR 8062	*An Introduction to Privacy Engineering and Risk Management in Federal Systems*	January 2017
NISTIR 8011 Volume 1	*Automation Support for Security Control Assessments: Overview*	June 2017
NISTIR 8011 Volume 2	*Automation Support for Security Control Assessments: Hardware Asset Management*	June 2017
NISTIR 7621 Rev. 1	*Small Business Information Security: The Fundamentals*	November 2016

ITL BULLETINS

TABLE 9: FY 2017 ITL BULLETINS	
PUBLICATION DATE	**BULLETIN TITLE**
September 2017	*Updating the Keys for DNS Security*
August 2017	*Understanding the Major Update to NIST SP 800-63: Digital Identity Guidelines*
July 2017	*Updated NIST Guidance for Bluetooth Security*
June 2017	*Toward Standardizing Lightweight Cryptography*
May 2017	*Cyber-Threat Intelligence and Information Sharing*
April 2017	*Building the Bridge Between Privacy and Cybersecurity for Federal Systems*
March 2017	*Fundamentals of Small Business Information Security*
February 2017	*Guide for Cybersecurity Incident Recovery*
January 2017	*Dramatically Reducing Software Vulnerabilities*
December 2016	*Rethinking Security Through Systems Security Engineering*
November 2016	*Exploring the Next Generation of Access Control Methodologies*
October 2016	*Making Email Trustworthy*

OTHER NIST PUBLICATIONS

NIST released other publications in FY 2017, as "White Papers," and as Concept Papers and Project Descriptions from NCCoE.

TABLE 10: OTHER FY 2017 PUBLICATIONS

PUBLICATION TYPE	PUBLICATION TITLE	RELEASE DATE
Project Description (Final) (Draft)	*Capabilities Assessment for Securing Manufacturing Industrial Control Systems*	March 2017 November 2016
Project Description (Final)	*Mobile Application Single Sign-On: for Public Safety and First Responders*	November 2016
Project Description (Final) (Draft)	*Secure Inter-Domain Routing--Part 1: Route Hijacks*	July 2017 May 2017
Project Description (Final) (Draft)	*Securing Property Management Systems: Cybersecurity for the Hospitality Sector*	September 2017 April 2017
Project Description (Draft)	*Trusted Geolocation in the Cloud*	May 2017
White Paper (Final)	*Baldrige Cybersecurity Excellence Builder: Key questions for improving your organization's cybersecurity performance*	April 2017
White Paper (Draft)	*Cybersecurity Framework Manufacturing Profile*	March 2017
White Paper (Draft)	*Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*	January 2017
White Paper (Draft)	*Profiles for the Lightweight Cryptography Standardization Process*	April 2017

ITL CYBERSECURITY PROGRAM RELATED PUBLICATIONS

NIST Technical Series Publications and Other NIST Publications

The tables above list NIST Technical Series cybersecurity publications posted by ITL—either as draft or final publications—during FY 2017 (from October 1, 2016 to September 30, 2017). Abstracts and links to the full text of these publications are provided in the sections that follow.

During FY 2017, the ITL staff authored a significant number of standards, guidelines, recommendations and other research papers related to cybersecurity. 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), as other NIST publications, or as externally-published documents (e.g., journal articles, conference papers, books, and other papers).

In FY 2017, ITL published 20 NIST Special Publications, 10 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 21 Special Publications, 5 NISTIRs, 4 NCCoE Project Descriptions, and 4 NIST "white papers." ITL research was also published externally as 15 journal articles, 17 conference papers and 2 external "white papers." They are listed in the following sections, with abstracts.

Top 10 Most Downloaded FIPS/SPs/NISTIRs – published in FY 2017

1. **SP 800-160**, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (54,557 downloads)
2. **SP 800-184**, *Guide for Cybersecurity Event Recovery* (49,929)
3. **SP 800-63-3**, *Digital Identity Guidelines* (49,535)
4. **SP 800-171 Rev. 1**, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (43,552)
5. **NISTIR 7621 Rev. 1,** *Small Business Information Security: The Fundamentals* (42,912)
6. **SP 800-63B**, *Digital Identity Guidelines: Authentication and Lifecycle Management* (40,152)
7. **NISTIR 8151**, *Dramatically Reducing Software Vulnerabilities: Report to the White House Office of Science and Technology Policy* (34,868)
8. **SP 800-181**, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (31,782)
9. **SP 800-179**, *Guide to Securing Apple OS X 10.10 Systems for IT Professionals: A NIST Security Configuration Checklist* (25,851)
10. **SP 800-63A**, *Digital Identity Guidelines: Enrollment and Identity Proofing* (14,699)

Top 10 Most-Downloaded FIPS/SPs/NISTIRs – all years

1. **SP 800-53 Rev. 4**, *Security and Privacy Controls for Federal Information Systems and Organizations* (376,759 downloads)
2. **SP 800-61 Rev. 2**, *Computer Security Incident Handling Guide* (185,976)
3. **SP 800-145**, *The NIST Definition of Cloud Computing* (147,801)
4. **SP 800-171**, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* (147,208)

5. **SP 800-30 Rev. 1**, *Guide for Conducting Risk Assessments* (112,526)
6. **SP 800-88 Rev. 1**, *Guidelines for Media Sanitization* (77,150)
7. **SP 800-82 Rev. 2**, *Guide to Industrial Control Systems (ICS) Security* (66,663)
8. **SP 800-53A Rev. 4**, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans* (65,389)
9. **NISTIR 7298 Rev. 2**, *Glossary of Key Information Security Terms* (57,689)
10. **SP 800-160**, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* (54,557)

FY 2018 Plans

The Computer Security Division will leverage the capabilities of the new CSRC platform to enhance the searching and browsing functionality of the website's publications section. The CSRC development team will also explore ways to improve the automated sharing of publication information with other NIST offices. Finally, NIST will continue to expand its library of cybersecurity and privacy publications, both through NIST technical publication series and external publishing opportunities.

FOR MORE INFORMATION, SEE:

https://csrc.nist.gov/publications

CONTACTS:

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

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

Abstracts of Publications Released in FY 2017

The following sections provide abstracts of security- and privacy-related NIST Special Publications (SP), NIST Internal or Interagency Reports (NISTIR), and other NIST publications listed in the previous section. If a publication was released as a draft *and* final publication during FY 2017, only the final publication is listed below. Any updated publications, with minor technical or editorial changes, identified in the tables above as "updates," are not listed below. Technical reports (SP and NISTIR series) are arranged in reverse numerical order by report number.

NIST SPECIAL PUBLICATIONS (SP) SP 800 SERIES – COMPUTER SECURITY

SP 800-195

2016 NIST/ITL Cybersecurity Program Annual Report

September 2017

https://csrc.nist.gov/publications/detail/sp/800-195/final

https://doi.org/10.6028/NIST.SP.800-195

Title III of the E-Government Act of 2002, entitled the Federal Information Security Management Act (FISMA) of 2002, requires NIST to prepare an annual public report on activities undertaken in the previous year, and planned for the coming year, to carry out responsibilities under this law. The primary goal of the NIST's Information Technology Laboratory (ITL) Cybersecurity Program, is to provide standards and technology that protects information systems against threats to the confidentiality, integrity, and availability of information and services. During Fiscal Year 2016 (FY 2016), the ITL Cybersecurity Program successfully responded to numerous challenges and opportunities in fulfilling that mission. Through ITL'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 ITL Cybersecurity Program was engaged during FY 2016.

SP 800-193 (DRAFT)

Platform Firmware Resiliency Guidelines

May 2017 (public comment period: May 30 – July 14, 2017)

https://csrc.nist.gov/publications/detail/sp/800-193/draft

This document provides technical guidelines and recommendations supporting the resiliency of platform firmware and data against potentially destructive attacks. The platform is a collection of the fundamental hardware and firmware components needed to boot and operate a system. A successful attack on platform firmware could render a system inoperable, perhaps permanently or requiring reprogramming by the original manufacturer, resulting in significant disruptions to users. The technical guidelines in this document promote resiliency in the platform by describing security mechanisms for protecting the platform against unauthorized changes, detecting unauthorized changes that occur, and recovery from attacks rapidly and securely. Implementers, including Original Equipment Manufacturers (OEMs) and component/device suppliers, can use these guidelines to build stronger security mechanisms into platforms. System administrators, security professionals, and users can use this document to guide procurement strategies and priorities for future systems.

SP 800-192

Verification and Test Methods for Access Control Policies/Models

June 2017

https://csrc.nist.gov/publications/detail/sp/800-192/final

https://doi.org/10.6028/NIST.SP.800-192

Access control systems are among the most critical of computer security components. Faulty policies, misconfigurations, or flaws in software implementations can result in serious vulnerabilities. To formally and precisely capture the security properties that access control should adhere to, access control models are usually written, bridging the gap in abstraction between policies and mechanisms. Identifying discrepancies between policy specifications and their intended function is crucial because correct implementation and enforcement of policies by applications is based on the premise that the policy specifications are correct. As a result, policy specifications represented by models must undergo rigorous verification and validation through systematic verification and testing to ensure that the policy specifications truly encapsulate the desires of the policy authors. Verifying the conformance of access control policies and models is a non-trivial and critical task, and one important aspect of such verification is to formally check the inconsistency and incompleteness of the model and safety requirements of the policy, because an access control model and its implementation do not necessarily explicitly express the policy, which can also be implicitly embedded by mixing with direct access constraints or other access control models.

SP 800-191 (DRAFT)

The NIST Definition of Fog Computing

August 2017 (public comment period: August 21 – September 21, 2017)

https://csrc.nist.gov/publications/detail/sp/800-191/draft

Managing the data generated by Internet of Things (IoT) sensors is one of the biggest challenges faced when deploying an IoT system. Traditional cloud-based IoT systems are challenged by the large scale, heterogeneity, and high latency witnessed in some cloud ecosystems. One solution is to decentralize applications, management, and data analytics into the network itself using a distributed and federated computing model. This approach has become known as fog computing. This document presents a formal definition of fog and mist computing and how they relate to cloud-based computing models for IoT. This document further characterizes important properties and aspects of fog computing, including service models, deployment strategies, and provides a baseline of what fog computing is, and how it may be used.

SP 800-190

Application Container Security Guide

September 2017 (also issued as two public drafts during FY 2017)

https://csrc.nist.gov/publications/detail/sp/800-190/final

https://doi.org/10.6028/NIST.SP.800-190

Application container technologies, also known as containers, are a form of operating system virtualization combined with application software packaging. Containers provide a portable, reusable, and automatable way to package and run applications. This publication explains the potential security concerns associated with the use of containers and provides recommendations for addressing these concerns.

SP 800-188 (2nd DRAFT)

De-Identifying Government Datasets

December 2016 (public comment period: December 15-31, 2016)

https://csrc.nist.gov/publications/detail/sp/800-188/draft

De-identification is a process that is applied to a dataset to reduce the risk of linking information revealed in the dataset to 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-Identification of Personal Information*, 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, or providing a query interface that incorporates de-identification of the identified data. Agencies can create 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, transforming quasi-identifiers and the use of formal privacy models. People performing de-identification generally use special-purpose software tools to perform the data manipulation and calculate the likely risk of re-identification. However, not all tools that merely 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 800-187 (DRAFT)

Guide to LTE Security

November 2017 (public comment period: November 21 – December 22, 2017)

https://csrc.nist.gov/publications/detail/sp/800-187/draft

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) Long Term Evolution (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.

SP 800-185

SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash

December 2016

https://csrc.nist.gov/publications/detail/sp/800-185/final

https://doi.org/10.6028/NIST.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 designed to hash tuples of input strings unambiguously. ParallelHash is a

variable-length hash function that can hash very long messages in parallel.

SP 800-184

Guide for Cybersecurity Event Recovery

December 2016

https://csrc.nist.gov/publications/detail/sp/800-184/final

https://doi.org/10.6028/NIST.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 development, 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 information systems.

SP 800-181

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

August 2017

https://csrc.nist.gov/publications/detail/sp/800-181/final

https://doi.org/10.6028/NIST.SP.800-181

This publication describes the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework), a reference structure that describes the interdisciplinary nature of the cybersecurity work. It serves as a fundamental reference resource for describing and sharing information about cybersecurity work and the knowledge, skills, and abilities (KSAs) needed to complete tasks that can strengthen the cybersecurity posture of an organization. As a common, consistent lexicon that categorizes and describes cybersecurity work, the NICE Framework improves communication about how to identify, recruit, develop, and retain cybersecurity talent. The NICE Framework is a reference source from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of cybersecurity workforce development, planning, training, and education.

SP 800-179

Guide to Securing Apple OS X 10.10 Systems for IT Professionals: A NIST Security Configuration Checklist

December 2016

https://csrc.nist.gov/publications/detail/sp/800-179/final

https://doi.org/10.6028/NIST.SP.800-179

This publication assists IT professionals in securing Apple OS X 10.10 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 800-178

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)

October 2016

https://csrc.nist.gov/publications/detail/sp/800-178/final

https://doi.org/10.6028/NIST.SP.800-178

The Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC) are very different Attribute Based Access Control (ABAC) 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 on various types of data services. However, the two standards differ with respect to the manner in which access control policies are specified and implemented. This

document describes XACML and NGAC, and then compares them with respect to five criteria. The goal of this publication is to help ABAC users and vendors make informed decisions when addressing future data service policy enforcement requirements.

SP 800-177 Revision 1 (DRAFT)

Trustworthy Email

September 2017 (public comment period: September 13 – October 13, 2017)
https://csrc.nist.gov/publications/detail/sp/800-177/rev-1/draft

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 Transport Layer Security (TLS) and 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 associated certificate and key distribution protocols.

SP 800-171 Revision 1

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

December 2016
https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
https://doi.org/10.6028/NIST.SP.800-171r1

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 800-160

Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems

November 2016
https://csrc.nist.gov/publications/detail/sp/800-160/final
https://doi.org/10.6028/NIST.SP.800-160

With the continuing frequency, intensity, and adverse consequences of cyber-attacks, disruptions, hazards, and other threats to federal, state, and local governments, the military, businesses, and the critical infrastructure, the need for trustworthy secure systems has never been more important to the long-term economic and national security interests of the United States. Engineering-based solutions are essential to managing the growing complexity, dynamicity, and interconnectedness of today's systems, as exemplified by cyber-physical systems and systems-of-systems, including the Internet of Things. This publication addresses the engineering-driven perspective and actions necessary to develop more defensible and survivable systems, inclusive of the machine, physical, and human components that compose the systems and the capabilities and services delivered by 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 methods, practices, and techniques into those systems and software engineering activities. The objective is to address security issues from the protection needs, concerns, and requirements of perspective stakeholders and to use established engineering processes to ensure that such needs, concerns, and requirements are addressed with appropriate fidelity and rigor, early and in a sustainable manner throughout the life cycle of the system.

SP 800-150

Guide to Cyber Threat Information Sharing

October 2016

https://csrc.nist.gov/publications/detail/sp/800-150/final

https://doi.org/10.6028/NIST.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 compromise; 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 the organization's overall cybersecurity practices.

SP 800-125A (2nd Draft)

Security Recommendations for Hypervisor Deployment

September 2017 (public comment period: September 14 – October 6, 2017)

https://csrc.nist.gov/publications/detail/sp/800-125a/draft

The Hypervisor is a piece of software that provides an abstraction of all physical resources (such as CPU, Memory, Network and Storage) and thus enables multiple computing stacks (basically made of an O/S and application programs, and optionally a middleware in some instances) called Virtual Machines (VMs) to be run on a single physical host. In addition, it may have the functionality to define a network within the single physical host (called a virtual network) to enable communication among the VMs resident on that host as well as with physical and virtual machines outside the host. With all this functionality, the hypervisor has the responsibility to mediate access to physical resources, provide run-time isolation among resident VMs and enable a virtual network that provides security-preserving communication flow among the VMs and between the VMs and the external network. To design a hypervisor with the core functionality described above, there are architectural options, with each option presenting a different size of Trusted Computing Base (TCB) and hence, a different degree of ease in providing the required security assurance. Hence, in providing security recommendations for the hypervisor, two different approaches have been adopted in this document – one approach based on architectural options that provide the ease of security assurance and the second approach based on configuration choices that form part of its core administrative functions such as the management of VMs, hypervisor host, hypervisor software and virtual networks.

SP 800-121 Revision 2

Guide to Bluetooth Security

May 2017

https://csrc.nist.gov/publications/detail/sp/800-121/rev-2/final

https://doi.org/10.6028/NIST.SP.800-121r2

Bluetooth wireless technology is an open standard for short-range radio frequency communication that is used primarily to establish wireless personal area networks (WPANs) that has been integrated into many types of business and consumer devices. This publication provides information on the security capabilities of Bluetooth and gives recommendations to organizations employing Bluetooth regarding how to secure those

wireless technologies effectively. The Bluetooth versions within the scope of this publication are versions 1.1, 1.2, 2.0 + Enhanced Data Rate (EDR), 2.1 + EDR, 3.0 + High Speed (HS), 4.0, 4.1, and 4.2. Versions 4.0 and later support the low energy feature of Bluetooth.

SP 800-70 Revision 4 (DRAFT)

National Checklist Program for IT Products: Guidelines for Checklist Users and Developers

August 2017 (public comment period: August 1-30, 2017)

https://csrc.nist.gov/publications/detail/sp/800-70/rev-4/draft

A security configuration checklist is a document that contains instructions or procedures for configuring an information technology (IT) product to 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 800-67 Revision 2 (DRAFT)

Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher

July 2017 (public comment period: July 18 – October 2, 2017)

https://csrc.nist.gov/publications/detail/sp/800-67/rev-2/draft

This publication specifies the Triple Data Encryption Algorithm (TDEA), including its primary component cryptographic engine, the Data Encryption Algorithm (DEA). When implemented in an SP 800-38-series-compliant mode of operation and in a FIPS 140-2-compliant cryptographic module, TDEA may be used by federal organizations to protect sensitive unclassified data. Protection of data during transmission or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by the data. This Recommendation defines the mathematical steps required to cryptographically protect data using TDEA and to subsequently process such protected data. TDEA is made available for use by federal agencies within the context of a total security program consisting of physical security procedures, good information management practices, and computer system/network access controls.

SP 800-63-3

Digital Identity Guidelines

June 2017

https://csrc.nist.gov/publications/detail/sp/800-63/3/final

https://doi.org/10.6028/NIST.SP.800-63-3

These guidelines provide technical requirements for federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose. The guidelines cover identity proofing and authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks. They define technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions. This publication supersedes SP 800-63-2.

SP 800-63A

Digital Identity Guidelines: Enrollment and Identity Proofing

June 2017

https://csrc.nist.gov/publications/detail/sp/800-63a/final

https://doi.org/10.6028/NIST.SP.800-63a

These guidelines provide technical requirements for federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose. This guideline focuses on the enrollment and verification of an identity for use in digital authentication. Central to this is a process known as identity proofing in which applicants provide evidence to a credential service provider (CSP) that reliably identifies them, thereby allowing the CSP to assert that identification is at a useful identity assurance level. This document defines technical

requirements for each of three identity assurance levels. This publication supersedes corresponding sections of SP 800-63-2.

SP 800-63B

Digital Identity Guidelines: Authentication and Lifecycle Management

June 2017

https://csrc.nist.gov/publications/detail/sp/800-63b/final

https://doi.org/10.6028/NIST.SP.800-63b

These guidelines provide technical requirements for federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose. These guidelines focus on the authentication of subjects interacting with government systems over open networks, establishing that a given claimant is a subscriber who has been previously authenticated. The result of the authentication process may be used locally by the system performing the authentication or may be asserted elsewhere in a federated identity system. This document defines technical requirements for each of the three authenticator assurance levels. This publication supersedes corresponding sections of SP 800-63-2.

SP 800-63C

Digital Identity Guidelines: Federation and Assertions

June 2017

https://csrc.nist.gov/publications/detail/sp/800-63c/final

https://doi.org/10.6028/NIST.SP.800-63c

This document and its companion documents, SP 800-63, SP 800-63A, and SP 800-63B, provide technical and procedural guidelines to agencies for the implementation of federated identity systems and for assertions used by federations. This publication supersedes corresponding sections of SP 800-63-2. These guidelines provide technical requirements for federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose. This guideline focuses on the use of federated identity and the use of assertions to implement identity federations. Federation allows a given credential service provider to provide authentication and (optionally) subscriber attributes to a number of separately-administered relying parties. Similarly, relying parties may use more than one credential service provider.

SP 800-56C Revision 1 (DRAFT)

Recommendation for Key Derivation Methods in Key-Establishment Schemes

August 2017 (public comment period: August 7 – November 6, 2017)

https://csrc.nist.gov/publications/detail/sp/800-56c/rev-1/draft

This Recommendation specifies techniques for the derivation of keying material from a shared secret established during a key-establishment scheme defined in SP 800-56A or SP 800-56B.

SP 800-56A Revision 3 (DRAFT)

Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography

August 2017 (public comment period: August 7 – November 6, 2017)

https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/draft

This Recommendation specifies key-establishment schemes based on the discrete logarithm problem over finite fields and elliptic curves, including several variations of Diffie-Hellman and Menezes-Qu-Vanstone (MQV) key-establishment schemes.

SP 800-53 Revision 5 (DRAFT)

Security and Privacy Controls for Information Systems and Organizations

August 2017 (public comment period: August 15 – September 12, 2017)

https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

This publication provides a catalog of security and privacy controls for federal information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the nation from a diverse set of threats including hostile attacks, natural disasters, structural failures, human errors, and privacy risks. The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk. The

controls address diverse requirements derived from mission and business needs, laws, Executive Orders, directives, regulations, policies, standards, and guidelines. The publication describes how to develop specialized sets of controls, or overlays that are tailored for specific types of missions and business functions, technologies, environments of operation, and sector-specific applications. Finally, the consolidated catalog of controls addresses security and privacy from a functionality perspective (i.e., the strength of functions and mechanisms) and an assurance perspective (i.e., the measure of confidence in the security or privacy capability). Addressing both functionality and assurance ensures that information technology products and the information systems that rely on those products are sufficiently trustworthy.

SP 800-37 Revision 2 (Discussion Draft)
Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
September 2017
https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/draft

This publication provides guidelines for applying the Risk Management Framework (RMF) to information systems and organizations. The RMF includes a disciplined, structured, and flexible process for organizational asset valuation; security and privacy control selection, implementation, and assessment; system and control authorizations; and continuous monitoring. It also includes enterprise-level activities to better prepare organizations to execute the RMF at the system level. The RMF promotes the concept of near real-time risk management and ongoing system authorization through the implementation of continuous monitoring processes; provides senior leaders and executives with the necessary information to make cost-effective, risk management decisions about the systems supporting their missions and business functions; and integrates security and privacy controls into the system development life cycle. Applying the RMF tasks enterprise-wide helps to link essential risk management processes at the system level to risk management processes at the organization level. In addition, it establishes responsibility and accountability for the security and privacy controls deployed within organizational systems and inherited by those systems. The RMF incorporates concepts from the Framework for Improving Critical Infrastructure Cybersecurity that complements the currently established risk management processes mandated by the Office of Management and Budget and the Federal Information Security Modernization Act.

SP 800-12 Revision 1
An Introduction to Information Security
June 2017
https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final
https://doi.org/10.6028/NIST.SP.800-12r1

Organizations rely heavily on the use of information technology (IT) products and services to run their day-to-day activities. Ensuring the security of these products and services is of the utmost importance for the success of the organization. This publication introduces the information security principles that organizations may leverage to understand the information security needs of their respective systems.

SP 1800 SERIES – CYBERSECURITY PRACTICE GUIDES

SP 1800-12 (DRAFT)
Derived Personal Identity Verification (PIV) Credentials
September 2017 (public comment period: September 29 – November 29, 2017)
https://nccoe.nist.gov/projects/building-blocks/piv-credentials

Federal Information Processing (FIPS) Standards Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, establishes a standard for a PIV system based on secure and reliable forms of identity credentials that are issued by the Federal Government to its employees and contractors. These credentials are intended to authenticate individuals who require access to federally controlled facilities, information systems, and applications.

In 2005, when FIPS 201 was first published, logical access was geared toward traditional computing devices (i.e., desktop and laptop computers), where the PIV card provides common authentication mechanisms through integrated smart card readers across the Federal Government. With the emergence of computing devices such as tablets, convertible computers, and, in particular, mobile devices, the use of PIV cards has proved challenging. Mobile devices lack the integrated smart card readers found in laptop and desktop computers and require separate card readers attached to devices to provide authentication services. To extend the value of PIV systems into mobile devices that do not have PIV Card readers, NIST developed technical guidelines on the implementation or lifecycle of identity credentials that are issued by federal departments and agencies to individuals who possess and prove control over a valid PIV card.

These NIST guidelines, published in 2014, describe Derived PIV Credentials (DPCs), which leverage the identity proofing and vetting results of current and valid PIV credentials. To demonstrate the DPC's guidelines, the NCCoE at NIST built a security architecture in its laboratory using commercial technology to manage the lifecycle of DPCs, demonstrating the process that enables a PIV Card holder to establish DPCs in a mobile device that then can be used to allow the PIV Card holder to access websites that require PIV authentication. This project resulted in a freely available NIST Cybersecurity Practice Guide that demonstrates how an organization can continue to provide two-factor authentication for users with a mobile device that leverages the strengths of the PIV standard. Although this project is primarily aimed at the federal sector's needs, it is also relevant to mobile device users with smart card based credentials in the private sector.

SP 1800-11 (DRAFT)

Data Integrity: Recovering from Ransomware and Other Destructive Events

September 2017 (public comment period: September 6 – November 6, 2017)
https://nccoe.nist.gov/projects/building-blocks/data-integrity

Businesses face a near-constant threat of destructive malware, ransomware, malicious insider activities, and even honest mistakes that can alter or destroy critical data. These data corruption events could cause a significant loss to a company's reputation, business operations, and bottom line. These types of adverse events that ultimately impact data integrity can compromise critical corporate information, including emails, employee records, financial records, and customer data. It is imperative for organizations to recover quickly from a data integrity attack and trust the accuracy and precision of the recovered data. The NCCoE at NIST built a laboratory environment to explore methods to effectively recover from a data corruption event in various Information Technology (IT) enterprise environments. NCCoE also implemented the auditing and reporting IT system use to support incident recovery and investigations. This NIST Cybersecurity Practice Guide demonstrates how organizations can implement technologies to take immediate action following a data corruption event. The example solution outlined in this guide encourages the effective monitoring and detection of data corruption in standard, enterprise components as well as custom applications and data composed of open-source and commercially available components.

SP 1800-9 (DRAFT)

Access Rights Management for the Financial Services Sector

August 2017 (public comment period: August 31 – October 31, 2017)
https://nccoe.nist.gov/projects/use-cases/access-rights-management

Managing access to resources (data) is complicated because internal systems multiply and acquisitions add to the complexity of an organization's IT infrastructure. Identity and access management (IdAM) is the set of technology, policies, and processes that are used to manage access to resources. Access rights management (ARM) is the subset of those technologies, policies, and processes that manage the rights of individuals and systems to access resources (data). In other words, an ARM system enables a company to give the right person the right access to the right resources at the right time.

The goal of this project is to demonstrate an ARM solution that is a standards-based technical

approach to coordinating and automating updates to and improving the security of the repositories (directories) that maintain the user access information across an organization. The coordination improves cybersecurity by ensuring that user access information is updated accurately (according to access policies), including disabling accounts or revoking access privileges as user resource access needs change. Cybersecurity is also improved through better monitoring for unauthorized changes (e.g., privilege escalation). The system executes user access changes across the enterprise according to corporate access policies quickly, simultaneously, and consistently.

The ARM reference design and example implementation are described in this NIST Cybersecurity "Access Rights Management" practice guide. This project resulted from discussions among NCCoE staff and members of the financial services sector. This NIST Cybersecurity Practice Guide also describes our collaborative efforts with technology providers and financial services stakeholders to address the security challenges of ARM. It provides a modular, open, end-to-end example implementation that can be tailored to financial services companies of varying sizes and sophistication. The use case scenario that provides the underlying impetus for the functionality presented in the guide is based on normal day-to-day business operations. Although the reference solution was demonstrated with a certain suite of products, the guide does not endorse these specific products. Instead, it presents the NIST Cybersecurity Framework (CSF) core functions and subcategories, as well as the financial industry guidelines that a company's security personnel can use to identify similar standards-based products that can be integrated quickly and cost-effectively with a company's existing tools and infrastructure.

Planning for the deployment of the design gives an organization the opportunity to review and audit the access control information in their directories and get a more global, correlated, disambiguated view of the user access roles and attributes that are currently in effect.

SP 1800-8 (DRAFT)
Securing Wireless Infusion Pumps in Healthcare Delivery Organizations
May 2017 (public comment period: May 8 – July 7, 2017)
https://nccoe.nist.gov/projects/use_cases/medical_devices

Medical devices, such as infusion pumps, were once standalone instruments that interacted only with the patient or medical provider. But today's medical devices connect to a variety of health care systems, networks, and other tools within a healthcare delivery organization (HDO). Connecting devices to point-of-care medication systems and electronic health records can improve healthcare delivery processes; however, increasing the connectivity capabilities also creates cybersecurity risks. Potential threats include unauthorized access to patient health information, changes to prescribed drug doses, and interference with a pump's function.

The NCCoE at NIST analyzed risk factors in and around the infusion pump ecosystem using a questionnaire-based risk assessment to develop an example implementation that demonstrates how HDOs can use standards-based, commercially available cybersecurity technologies to better protect the infusion pump ecosystem, including patient information and drug library dosing limits. This practice guide will help HDOs implement current cybersecurity standards and best practices to reduce their cybersecurity risk, while maintaining the performance and usability of wireless infusion pumps.

SP 1800-7 (DRAFT)
Situational Awareness for Electric Utilities
February 2017 (public comment period: February 16 – April 17, 2017)
https://nccoe.nist.gov/projects/use_cases/situational_awareness

This NIST Cybersecurity Practice Guide describes our collaborative efforts with technology providers and energy-sector stakeholders to address the security challenges that energy providers face in deploying a comprehensive situational awareness capability. It offers a technical approach to meeting the challenge, and also incorporates a business-value mind-set by identifying the strategic considerations involved in implementing new technologies. The guide provides a modular,

end-to-end example solution that can be tailored and implemented by energy providers of varying sizes and sophistication. It shows energy providers how we met the challenge using open source and commercially available tools and technologies that are consistent with cybersecurity standards. The use case is based on an everyday operational business scenario that provides the underlying impetus for the functionality presented in the guide. Test cases were defined with industry participation to provide multiple examples of the capabilities necessary to provide situational awareness.

SP 1800-6 (DRAFT)

Domain Name Systems-Based Electronic Mail Security

November 2016 (public comment period: November 2 – December 19, 2016)
https://nccoe.nist.gov/projects/building-blocks/secured-email

This document proposes a reference guide on how to architect, install, and configure a security platform for trustworthy email exchanges across organizational boundaries. The project includes reliable authentication of mail servers, digitally signing and encrypting email, and binding cryptographic key certificates to sources and servers. The example solutions and architectures presented are based upon standards-based and commercially available products. The example solutions presented can be used by any organization implementing Domain Name System-based electronic mail security.

SP 1800-3 (2nd DRAFT)

Attribute Based Access Control

September 2017 (public comment period: September 20 – October 20, 2017)
https://nccoe.nist.gov/projects/building-blocks/attribute-based-access-control

Enterprises rely upon strong access control mechanisms to ensure that corporate resources (e.g., applications, networks, systems, and data) are not exposed to anyone other than an authorized user. As business requirements change, enterprises need highly flexible access control mechanisms that can adapt. The application of attribute based policy definitions enables enterprises to accommodate a diverse set of business cases. This NCCoE practice guide details a collaborative effort between the NCCoE and technology providers to demonstrate a standards-based approach to Attribute Based Access Control (ABAC). This guide discusses potential security risks facing organizations, benefits that may result from the implementation of an ABAC system, and the approach that the NCCoE took in developing a reference architecture and build. It includes a discussion of major architecture design considerations, an explanation of security characteristics achieved by the reference design, and a mapping of the security characteristics to applicable standards and security control families. For parties interested in adopting all or part of the NCCoE reference architecture, this guide includes a detailed description of the installation, configuration, and integration of all components.

SP 500 SERIES—COMPUTER SYSTEMS TECHNOLOGY

SP 500-320

Report of the Workshop on Software Measures and Metrics to Reduce Security Vulnerabilities (SwMM-RSV)

November 2016
https://doi.org/10.6028/NIST.SP.500-320

The NIST workshop on Software Measures and Metrics to Reduce Security Vulnerabilities (SwMM-RSV) was held on 12 July 2016. The goal of this workshop was to gather ideas on how the Federal Government can identify, improve, package, deliver, or boost the use of software measures and metrics to significantly reduce vulnerabilities.

This report contains observations and recommendations from the workshop participants and includes position statements submitted to the workshop, presentations at the workshop, and related material. Ideas from the workshop were included in the *Dramatically Reducing Software Vulnerabilities* report, requested of NIST by the White House Office of Science and Technology Policy in Spring 2016.

NIST INTERNAL / INTERAGENCY REPORTS (NISTIR)

NISTIR 8192

Enhancing Resilience of the Internet and Communications Ecosystem: a NIST Workshop Proceedings

September 2017

https://csrc.nist.gov/publications/detail/nistir/8192/final

https://doi.org/10.6028/NIST.IR.8192

These proceedings document the July 11-12, 2017 "Enhancing Resilience of the Internet and Communications Ecosystem" workshop led by the National Institute of Standards and Technology. Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" required the Secretaries of Commerce and Homeland Security to "jointly lead an open and transparent process to identify and promote action by appropriate stakeholders to improve the resilience of the Internet and communications ecosystem, and to encourage collaboration with the goal of dramatically reducing threats perpetrated by automated and distributed attacks (e.g., botnets)." The workshop was designed to allow stakeholders to explore a range of current and emerging solutions addressing automated, distributed threats in an open and transparent manner. The workshop attracted 150 participants from diverse stakeholder communities and was conducted under Chatham House Rules.

NISTIR 8183

Cybersecurity Framework Manufacturing Profile

September 2017

https://csrc.nist.gov/publications/detail/nistir/8183/final

https://doi.org/10.6028/NIST.IR.8183

This document provides the NIST Cybersecurity Framework (CSF) 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. This Manufacturing Profile provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to manufacturing systems. The Manufacturing Profile is meant to enhance but not replace current cybersecurity standards and industry guidelines that the manufacturer is embracing.

NISTIR 8179 (DRAFT)

Criticality Analysis Process Model: Prioritizing Systems and Components

July 2017 (public comment period: July 10 – August 18, 2017)

https://csrc.nist.gov/publications/detail/nistir/8179/draft

In the modern world where complex systems and systems-of-systems are integral to the functioning of society and businesses, it is increasingly important to be able to understand and manage risks that these systems and components may present to the missions that they support. However, in the world of finite resources, it is not possible to apply equal protection to all assets. This publication describes a comprehensive Criticality Analysis Process Model – a structured method of prioritizing programs, systems, and components based on their importance to the goals of an organization and the impact that their inadequate operation or loss may present to those goals. A criticality analysis can help organizations identify and better understand the systems, subsystems, components and subcomponents that are most essential to their operations and the environment in which they operate. That understanding facilitates better decision making related to the management of an organization's information assets, including information security risk management, project management, acquisition, maintenance, and upgrade decisions. The Model is structured to logically follow how organizations design and implement projects and systems, can be used as a component of a holistic and comprehensive risk management approach that considers all risks, and can be used with a variety of risk management standards and guidelines.

NISTIR 8176 (DRAFT)

Security Assurance Challenges for Container Deployment

August 2017 (public comment period: August 1-25, 2017)

https://csrc.nist.gov/publications/detail/nistir/8176/draft

Application containers are slowly being adopted in enterprise IT infrastructures. Security guidelines and countermeasures have been proposed to address the security concerns associated with the deployment of application container platforms. To assess the effectiveness of the security solutions implemented based on these recommendations, it is necessary to analyze the solutions and outline the security assurance requirements they must satisfy to meet their intended objectives. This is the contribution of this document. The focus is on application containers on a Linux platform.

NISTIR 8170 (DRAFT)

The Cybersecurity Framework: Implementation Guidance for Federal Agencies

May 2017 (public comment period: May 12 – June 30, 2017)

https://csrc.nist.gov/publications/detail/nistir/8170/draft

This publication assists federal agencies in strengthening their cybersecurity risk management by helping them to determine an appropriate implementation of the Framework for Improving Critical Infrastructure Cybersecurity (known as the Cybersecurity Framework). Federal agencies can use the Cybersecurity Framework to complement the existing suite of NIST security and privacy risk management standards, guidelines, and practices developed in response to the Federal Information Security Management Act, as amended (FISMA). The relationship between the Cybersecurity Framework and the National Institute of Standards and Technology (NIST) Risk Management Framework are discussed in eight use cases.

NISTIR 8165

Impact of Code Complexity on Software Analysis

February 2017

https://csrc.nist.gov/publications/detail/nistir/8165/final

https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8165.pdf

The Software Assurance Metrics and Tool Evaluation (SAMATE) team studied thousands of warnings from static analyzers. Tools have difficulty distinguishing between the absence of a weakness and the presence of a weakness that is buried in otherwise-irrelevant code elements. This paper presents classes of these code elements, which we call "code complexities."

These code elements have been present in software assurance testing regimens as part of the generation strategy for test cases when evaluating static analyzers. The benefits of using code complexity include the development of coding guidelines, boosting the diversification of the test cases.

NISTIR 8151

Dramatically Reducing Software Vulnerabilities: Report to the White House Office of Science and Technology Policy

November 2016

https://csrc.nist.gov/publications/detail/nistir/8151/final

https://doi.org/10.6028/NIST.IR.8151

The call for a dramatic reduction in software vulnerability is heard from multiple sources, recently from the February 2016 Federal Cybersecurity Research and Development Strategic Plan. This plan starts by describing well-known risks; current systems perform increasingly vital tasks and are widely known to possess vulnerabilities. These vulnerabilities are often not easy to discover and are difficult to correct. Cybersecurity has not kept pace, and the pace that is needed is rapidly accelerating. The goal of this report is to present a list of specific technical approaches that have the potential to make a dramatic difference in reducing vulnerabilities – by stopping them before they occur, by finding them before they are exploited or by reducing their impact.

NISTIR 8139 (DRAFT)

Identifying Uniformity with Entropy and Divergence

February 2017 (public comment period: February 2 – March 9, 2017)

https://csrc.nist.gov/publications/detail/nistir/8139/draft

Entropy models are frequently utilized in tests identifying either the qualities of randomness or the randomness uniformity of formal and/or observed distributions. SP 800-22 and SP 800-90 (A, B, and C) discuss tests and methods leveraging both Shannon and min entropies. Shannon and min entropies represent two particular cases of Renyi entropy, which is a more general, one-parameter entropy model. Renyi entropy insightfully unifies Hartley, Shannon, collision, and min entropies and belongs to the class of one parameter entropy models, such as entropies named after Havrda-Charvat-Daroczy, Tsallis, Abe, and Kaniadakis. Renyi entropy, along with the other members of the one-parameter entropy models class, can be viewed as a case of the Sharma-Mittal entropy, which is a bi-parametric generalized entropy model. This NISTIR focuses on using Renyi and Tsallis entropy and divergence models to analyze similarities and differences between the probability distributions of interest. The report introduces extensions for the traditional uniformity identification and measurement techniques that were proposed in SP 800-22 and SP 800-90.

NISTIR 8136

An Overview of Mobile Application Vetting Services for Public Safety

January 2017

https://csrc.nist.gov/publications/detail/nistir/8136/final

https://doi.org/10.6028/NIST.IR.8136

The Middle Class Tax Relief Act of 2012 mandated the creation of the 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 are an important resource that will be utilized by this network. However, current mobile application developers may not be aware of 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. This document is intended to be an overview of existing mobile application vetting services, the features these services provide and how they relate to public safety's needs. It is also meant to aid public safety organizations when choosing which mobile application vetting services are used to evaluate relevant mobile applications.

NISTIR 8114

Report on Lightweight Cryptography

March 2017

https://csrc.nist.gov/publications/detail/nistir/8114/final

https://doi.org/10.6028/NIST.IR.8114

The current NIST-approved cryptographic standards were designed to perform well on 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 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 8062

An Introduction to Privacy Engineering and Risk Management in Federal Systems

January 2017

https://csrc.nist.gov/publications/detail/nistir/8062/final

https://doi.org/10.6028/NIST.IR.8062

This document provides an introduction to the concepts of privacy engineering and risk management for federal systems. These concepts establish the basis for a common vocabulary to facilitate a better understanding and communication of privacy risks within federal systems and the effective implementation of privacy principles. This publication introduces two key components to support the application of privacy engineering and risk management: privacy engineering objectives and a privacy risk model.

NISTIR 8011 Volume 1

Automation Support for Security Control Assessments: Overview

June 2017

https://csrc.nist.gov/publications/detail/nistir/8011/vol-1/final

https://doi.org/10.6028/NIST.IR.8011-1

This volume introduces concepts to support the automated assessment of most of the security controls in SP 800-53. Referencing SP 800-53A, the controls are divided into more granular parts (called determination statements) to be assessed. The parts of the control assessed by each determination statement are called control items. The 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).

NISTIR 8011 Volume 2

Automation Support for Security Control Assessments: Hardware Asset Management

June 2017

https://csrc.nist.gov/publications/detail/nistir/8011/vol-2/final

https://doi.org/10.6028/NIST.IR.8011-2

The NISTIR 8011 volumes focus on each individual information security capability, adding tangible detail to the more general overview given in NISTIR 8011 Volume 1, and providing a template for transition to a detailed, NIST standards-compliant automated assessment. 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 the risks created by unmanaged and/or unauthorized 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 7621 Revision 1

Small Business Information Security: The Fundamentals

November 2016

https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final

https://doi.org/10.6028/NIST.IR.7621r1

NIST developed this interagency report as a reference guideline about cybersecurity for small businesses. This document is intended to present the fundamentals of a small business information security program in non-technical language.

ITL BULLETINS

Building the Bridge Between Privacy and Cybersecurity for Federal Systems

April 2017

https://csrc.nist.gov/publications/detail/itl-bulletin/2017/04/building-bridge-b/w-privacy--cybersecurity-for-federal-systems/final

This bulletin summarizes the information in NISTIR 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Information Systems*, which provides an introduction to the concepts of privacy engineering and risk management for federal information systems. NISTIR 8062 introduces two key components to support the application of privacy engineering and risk management: privacy engineering objectives and a privacy risk model.

Cyber-Threat Intelligence and Information Sharing

May 2017

https://csrc.nist.gov/publications/detail/itl-bulletin/2017/05/cyber-threat-intelligence-and-information-sharing/final

This bulletin, based on SP 800-150, *Guide to Cyber Threat Information Sharing*, introduces cyber threat intelligence and information sharing concepts, describes the benefits and challenges of sharing, clarifies the importance of trust, and

introduces specific data handling considerations. It also describes how cyber threat intelligence and information sharing can help increase the efficiency and effectiveness of an organization's cybersecurity capabilities.

Dramatically Reducing Software Vulnerabilities

January 2017
https://csrc.nist.gov/publications/detail/itl-bulletin/2017/01/dramatically-reducing-software-vulnerabilities/final

This bulletin summarized the information presented in NISTIR 8151, *Dramatically Reducing Software Vulnerabilities: Report to the White House Office of Science and Technology Policy*. The publication starts by describing well-known security risks and presents a list of specific technical approaches that have the potential to make a dramatic difference in reducing vulnerabilities.

Exploring the Next Generation of Access Control Methodologies

November 2016
https://csrc.nist.gov/publications/detail/itl-bulletin/2016/11/exploring-the-next-generation-of-ac-methodologies/final

This bulletin summarizes the information presented in SP 800-178, *A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications*. The publication describes the Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC), and then compares them with respect to five criteria. The goal of this publication is to help ABAC users and vendors make informed decisions when addressing future data service policy enforcement requirements.

Fundamentals of Small Business Information Security

March 2017
https://csrc.nist.gov/publications/detail/itl-bulletin/2017/03/fundamentals-of-small-business-information-security/final

This bulletin summarizes the information in NISTIR 7621, Revision 1, *Small Business Information Security: The Fundamentals*. The bulletin presents the fundamentals of a small business information security program.

Guide for Cybersecurity Incident Recovery

February 2017
https://csrc.nist.gov/publications/detail/itl-bulletin/2017/02/guide-for-cybersecurity-incident-recovery/final

This bulletin summarizes the information presented in SP 800-184, *Guide for Cybersecurity Event Recovery*. The publication provides organizations with strategic guidance for planning, playbook developing, testing and improvements of recovery planning following a cybersecurity event.

Making Email Trustworthy

October 2016
https://csrc.nist.gov/publications/detail/itl-bulletin/2016/10/making-email-trustworthy/final

This bulletin summarizes the information presented in SP 800-177, *Trustworthy Email*. This publication gives recommendations and guidelines for enhancing trust in email. This guideline applies to federal IT systems and will also be useful for any small or medium sized organizations.

Rethinking Security Through Systems Security Engineering

December 2016
https://csrc.nist.gov/publications/detail/itl-bulletin/2016/12/rethinking-security-through-systems-security-engineering/final

This bulletin summarizes the information presented in SP 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. The publication addresses the engineering-driven perspective and actions necessary to develop more defensible and survivable systems, inclusive of the machine, physical, and human components that compose the systems and the capabilities and services delivered by those systems.

Toward Standardizing Lightweight Cryptography

June 2017
https://csrc.nist.gov/publications/detail/itl-bulletin/2017/06/toward-standardizing-lightweight-cryptography/final

This bulletin summarizes the information in NISTIR 8114, *Report on Lightweight Cryptography*, which provides an overview of the lightweight

cryptography project at NIST and describes plans for the standardization of lightweight cryptography algorithms.

Understanding the Major Update to NIST SP 800-63: Digital Identity Guidelines

August 2017
https://csrc.nist.gov/publications/detail/itl-bulletin/2017/08/update-nist-sp-800-63-digital-identity-guidelines/final

This bulletin outlines the updates that NIST recently made in its four-volume Special Publication (SP) 800-63, *Digital Identity Guidelines*, which provides agencies with technical guidelines regarding the digital authentication of users to federal networked systems.

Updated NIST Guidance for Bluetooth Security

July 2017
https://csrc.nist.gov/publications/detail/itl-bulletin/2017/07/updated-nist-guidance-for-bluetooth-security/final

This bulletin summarizes the information in SP 800-121 Revision 2, *Guide to Bluetooth Security*, which provides information on the security capabilities of Bluetooth and provides recommendations to organizations employing Bluetooth wireless technologies on securing them effectively.

Updating the Keys for DNS Security

September 2017
https://csrc.nist.gov/publications/detail/itl-bulletin/2017/09/updating-keys-for-dns-security/final

To help maintain the reliability and integrity of the Internet's Domain Name System (DNS), NIST is working with specialists from around the world to update the keys used by the DNS Security Extensions (DNSSEC) protocol to authenticate DNS data and avoid integrity issues such as domain name hijacking.

PROJECT DESCRIPTIONS (NCCOE)

Capabilities Assessment for Securing Manufacturing Industrial Control Systems:
Cybersecurity for Manufacturing

March 2017
https://nccoe.nist.gov/projects/use-cases/capabilities-assessment-securing-manufacturing-industrial-control-systems

Industrial Control Systems (ICS) monitor and control physical processes in many different industries and sectors. Cyber attacks against ICS devices present a real threat to organizations that employ ICS to monitor and control manufacturing processes. The NIST Engineering Laboratory (EL), in conjunction with the National Cybersecurity Center of Excellence, will produce a series of example solutions demonstrating four cybersecurity capabilities for manufacturing organizations. Each example solution will highlight an individual capability: Behavioral Anomaly Detection, ICS Application Whitelisting, Malware Detection and Mitigation, and ICS Data Integrity.

This capabilities assessment document is part one of a four-part series and addresses only behavioral anomaly detection capabilities. With these capabilities in place, manufacturers may find it easier to detect anomalous conditions, control what programs and applications are executed in their operating environments, mitigate malware attacks, and ensure the integrity of critical operational data. For each of the four capabilities listed above, the NIST EL and the NCCoE will map the security characteristics to the NIST Cybersecurity Framework (CSF), which will provide standards-based security controls for manufacturers. In addition, the EL and the NCCoE will implement each of the capabilities in two distinct but related lab settings: a robotics-based manufacturing enclave and a process control enclave that resembles what is being used by chemical manufacturing industries. This project will result in a publicly available NIST Cybersecurity Practice Guide, a detailed implementation guide of the practical steps needed to implement the cybersecurity example solution that addresses this challenge.

Mobile Application Single Sign-On: For Public Safety and First Responders

November 2016
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 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 will explore various multifactor authenticators currently in use by the public safety community, or those potentially offered in the future as their next generation networks are brought online. The effort will not only build an interoperable solution that can accept various authenticators to speed access to online systems while maintaining an appropriate amount of security, but will also focus 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 sets out to identify technical options for the public safety community to consider deploying to ensure that 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, detailing the technical decisions, trade-offs, lessons learned, and implementation 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.

Secure Inter-Domain Routing—Part 1: Route Hijacks
July 6, 2017
https://nccoe.nist.gov/projects/building-blocks/secure-inter-domain-routing

Since the creation of the Internet, the Border Gateway Protocol (BGP) has been the default routing protocol to route traffic among organizations (Internet Service Providers (ISPs) and Autonomous Systems (ASes)). While the BGP protocol performs adequately in identifying viable paths that reflect local routing policies and preferences to destinations, the lack of built-in security allows the protocol to be exploited. As a result, attacks against Internet routing functions are a significant and systemic threat to Internet-based information systems. The consequences of these attacks can: (1) deny access to Internet services; (2) detour Internet traffic to permit eavesdropping and to facilitate on-path attacks on endpoints (sites); (3) misdeliver Internet network traffic to malicious endpoints; (4) undermine IP address-based reputation and filtering systems; and (5) cause routing instability in the Internet.

To improve the security of inter-domain routing traffic exchange, NIST has begun the development of a Special Publication (SP 800-189 – in preparation) that provides security recommendations for the use of inter-domain protocols and routing technologies. These recommendations aim to protect the integrity of Internet traffic exchange. Implementing BGP Route Origin Validation (ROV) based upon the Resource Public Key Infrastructure (RPKI) can mitigate accidental and malicious attacks associated with route hijacking. The NCCoE understands that organizations and individuals have Internet performance expectations and requirements to protect against malicious cyber attacks. It is expected that eventual wide-scale deployment of RPKI-based ROV will significantly enhance the overall security and robustness of the Internet. This project will result in a NIST Cybersecurity Practice Guide—a publicly available description of the solution and practical steps needed to implement practices that effectively demonstrate the security and functionality of all components of ROV.

Securing Property Management Systems: Cybersecurity for the Hospitality Sector (DRAFT)
April 28, 2017
https://nccoe.nist.gov/projects/use_cases/securing-property-management-systems

Hospitality organizations rely on Property Management Systems (PMS) for daily tasks, planning, and record keeping. As the operations hub, the PMS interfaces with several services and components within a hotel's IT system, such as Point-of-Sale (POS) systems, door locks, Wi-Fi networks, and other guest service applications. Adding to

the complexity of connections, external business partners' components and services are also typically connected to the PMS, such as on-premise spas or restaurants, online travel agents, and customer relationship management partners or applications (on-premise or cloud-based). The numerous connections to, and users of the PMS, could provide a broader surface for attack by malicious actors. The draft describes methods to improve the security of the PMS, and how these methods can help protect the business from network intrusions that might lead to data breaches and fraud.

Based on industry research and in collaboration with hospitality industry stakeholders, the NCCoE is starting a project that aims to help hospitality organizations implement stronger security measures within and around the PMS, with a focus on the POS system through network segmentation, point-to-point encryption, data tokenization, multifactor authentication for remote and partner access, network and user behavior analytics, and business-only usage restrictions. In collaboration with the hospitality business community and technology vendors who implement standards that improve cybersecurity, the NCCoE will explore methods to strengthen the security of the PMS and its connections and will develop an example implementation composed of open-source and commercially available components. This project will produce a NIST Cybersecurity Practice Guide—a freely available description of the solution and practical steps needed to effectively secure the PMS and its many connections within the hotel IT system.

OTHER NIST PUBLICATIONS

Baldrige Cybersecurity Excellence Builder: Key questions for improving your organization's cybersecurity performance, v1.0

April 2017
https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative

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 your organization identify strengths and opportunities for improvement in managing cybersecurity risk based on your organization's mission, needs, and objectives. The *Baldrige Cybersecurity Excellence Builder* combines concepts in the *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) and the Baldrige Excellence Framework. Like those two sources, it is not a one-size-fits-all approach. It is adaptable and scalable to your organization's needs, goals, capabilities, and environment. It does not prescribe how you should structure your organization's cybersecurity policies and operations. Through interrelated sets of open-ended questions, it encourages you to use the approaches that best fit your organization. Using this self-assessment, you can:

- Determine cybersecurity-related activities that are important to your business strategy and critical service delivery;
- Prioritize your investments in managing cybersecurity risk;
- Determine how best to enable your 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 your use of cybersecurity standards, guidelines, and practices;
- Assess the cybersecurity results you achieve; and
- Identify strengths to leverage and priorities for improvement.

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (DRAFT)

January 10, 2017
https://www.nist.gov/file/344211

The national and economic security of the United States depends on the reliable functioning of its critical infrastructure. Cybersecurity threats take advantage of the increased complexity and connectivity of critical infrastructure systems, placing the nation's security at risk. To better protect these systems, the President issued Executive Order 13636, *Improving Critical Infrastructure*

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

Profiles for the Lightweight Cryptography Standardization Process (DRAFT)
April 2017
https://csrc.nist.gov/publications/detail/white-paper/2017/04/26/profiles-for-lightweight-cryptography-standardization-process/draft

This document describes the first two profiles for NIST's lightweight cryptography project. Profile I provides authenticated encryption with associated data (AEAD) and hashing functionalities for both hardware-oriented and software-oriented constrained environments. Profile II provides only AEAD in hardware-oriented constrained environments.

EXTERNAL PUBLICATIONS

The following journal articles and conference papers were published during FY 2017. For conference papers, the contributions listed below were either i) accepted for a conference held during FY 2017, or ii) accepted for a conference held prior to FY 2017 with final proceedings published in FY 2017 (and not listed in an earlier Annual Report). All NIST authors are identified using *italics*; publications are arranged alphabetically by author.

Links to document preprints are available at https://csrc.nist.gov/publications.

WHITE PAPERS

J. Alperin-Sheriff and D. Apon. **Tightly Secure Short Signatures from Weak PRFs**. Cryptology ePrint Archive, Report 2017/563, June 7, 2017, 26 pp.

http://ia.cr/2017/563

The Boyen-Li signature scheme [Asiacrypt'16] is a major theoretical breakthrough. Via a clever homomorphic evaluation of a pseudorandom function over their verification key, they achieve a reduction loss in security that is linear in the underlying security parameter and entirely independent of the number of message queries made, while still maintaining short signatures (consisting of a single short lattice vector). All previous schemes with such an independent reduction loss in security required a linear number of such lattice vectors, and even in the classical world, the only schemes achieving short signatures relied on non-standard assumptions.

We improve on their result, providing a verification key that is smaller by a linear factor, a significantly tighter reduction with only a constant loss, and signing and verification algorithms that could plausibly run in about 1 second. Our main idea is to change the scheme in a manner that allows us to replace the pseudorandom function evaluation with an evaluation of a much more efficient weak pseudorandom function.

As a matter of independent interest, we give

an improved method of the randomized inversion of the **G** gadget matrix, which reduces the noise growth rate in homomorphic evaluations performed in a large number of lattice-based cryptographic schemes, without incurring the high cost of sampling discrete Gaussian functions.

S. Breiner, J. Ross, and *C. Miller*. **Graphical Methods in Device-Independent Quantum Cryptography**. arXiv.org, Report 1705.09213, May 25, 2017, 15 pp.

https://arxiv.org/abs/1705.09213

We introduce a framework for graphical security proofs in device-independent quantum cryptography using the methods of categorical quantum mechanics. We are optimistic that this approach will make some of the highly complex proofs in quantum cryptography more accessible, facilitate the discovery of new proofs, and enable automated proof verification. As an example of our framework, we reprove a recent result from device-independent quantum cryptography: any linear randomness expansion protocol can be converted into an unbounded randomness expansion protocol. We give a graphical exposition of a proof of this result and implement parts of it in the Globular proof assistant.

JOURNAL ARTICLES

P. Black, *I. Bojanova*. **Defeating Buffer Overflow: A Trivial but Dangerous Bug.** *IT Professional* 18(6), pp. 58-61 (November/December 2016).

https://doi.org/10.1109/MITP.2016.117

With the C programming language comes buffer overflows. Because it is unlikely that the use of C will stop any time soon, the authors present some ways to deal with buffer overflows—both how to detect and how to prevent them.

L. Chen. **Cryptography Standards in Quantum Time: New Wine in an Old Wineskin?** *IEEE Security & Privacy* 15(4), pp. 51-57 (July/August 2017).

https://doi.org/10.1109/MSP.2017.3151339

The history of cryptography standards is reviewed, with a view to planning for the challenges, uncertainties, and strategies that the standardization of post-quantum cryptography will entail.

J. Chung, *M. Iorga*, *J. Voas* and S. Lee. **Alexa, Can I Trust You?** *Computer (IEEE Computer)* 50(9), pp. 100-104 (September 2017).

https://doi.org/10.1109/MC.2017.3571053

Several recent incidents highlight significant security and privacy risks associated with intelligent virtual assistants (IVAs). Better diagnostic testing of IVA ecosystems can reveal such vulnerabilities and lead to more trustworthy systems.

A.A. Ciss and *D. Moody*. **Geometric Progressions on Elliptic Curves**. *Glasnik Matematicki* 52(1), pp. 1-10 (2017).

https://web.math.pmf.unizg.hr/glasnik/vol_52/no1_01.html

In this paper, we look at long geometric progressions on different models of elliptic curves, namely Weierstrass curves, Edwards and twisted Edwards curves, Huff curves and general quartics curves. By a geometric progression on an elliptic curve, we mean the existence of rational points on the curve whose x-coordinates (or y-coordinates) are in geometric progression. We find infinite families of twisted Edwards curves and Huff curves with geometric progressions of length 5, an infinite family of Weierstrass curves with 8-term progressions, as well as infinite families of quartic curves containing 10-term geometric progressions.

F. Izadi, F. Khoshnam and *D. Moody*. **Heron Quadrilaterals via Elliptic Curves.** *Rocky Mountain Journal of Mathematics* 47(4), pp. 1227-1258 (2017).

https://doi.org/10.1216/RMJ-2017-47-4-1227

A Heron quadrilateral is a cyclic quadrilateral whose area and side lengths are rational. In this work, we establish a correspondence between Heron quadrilaterals and a family of elliptic curves of the form $y^2 = x^3 + ax^2 - n^2x$. This correspondence generalizes the notions of Goins and Maddox who established a similar connection between Heron triangles and elliptic curves. We further study this family of elliptic curves, looking at their torsion groups and ranks. We also explore their connection with the a=0 case of congruent numbers. Congruent

numbers are positive integers equal to the area of a right triangle with rational side lengths.

F. Khoshnam and *D. Moody*. **High Rank Elliptic Curves with Torsion $\mathbb{Z}/4\mathbb{Z}$ Induced by Kihara's Elliptic Curves**. *INTEGERS: The electronic journal of combinatorial number theory* 16, article no. A70, pp. 1-12 (October 5, 2016).

http://math.colgate.edu/~integers/vol16.html

Working over the field $\mathbb{Q}(t)$, Kihara constructed an elliptic curve with torsion group $\mathbb{Z}/4\mathbb{Z}$ and five independent rational points, showing that the rank is at least five. Following his approach, we give a new infinite family of elliptic curves with torsion group $\mathbb{Z}/4\mathbb{Z}$ and rank at least five. This matches the current record for such curves. In addition, we give specific examples of these curves with ranks 10 and 11.

D.R. Kuhn, *R.N. Kacker* and Y. Lei. **Measuring and Specifying Combinatorial Coverage of Test Input Configurations**. *Innovations in Systems and Software Engineering* 12(4), pp. 249-261 (December 2016).

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, *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.

N. Laplante, P. Laplante and *J. Voas*. **Caring: An Undiscovered Super "Ility" of Smart Healthcare**. *IEEE Software* 33(6), pp. 16-19 (November/December 2016).

https://doi.org/10.1109/MS.2016.136

As new and exciting healthcare applications arise that use smart technologies, the Internet of Things, data analytics, and other technologies, a critical problem is emerging: the potential loss of caring. Although these exciting technologies have improved patient care by allowing for better assessment, surveillance, and treatment, their use can disassociate the caregiver from the patient, essentially removing the "care" from healthcare. So, you can view caring as an undiscovered -ility that ranks at least as important as other well-known -ilities in healthcare systems.

P. Laplante, M. Kassab, N. Laplante and *J. Voas*. **Building Caring Healthcare Systems in the Internet of Things**. *IEEE Systems Journal* 99, pp. 1-8 (February 22, 2017).

https://doi.org/10.1109/JSYST.2017.2662602

The nature of healthcare and the computational and physical technologies and constraints present a number of challenges to systems designers and implementers. In spite of the challenges, there is a significant market for systems and products to support caregivers in their tasks as the number of people needing assistance grows substantially. In this paper, we present a structured approach for describing the Internet of Things (IoT) for healthcare systems. We illustrate the approach for three use cases and discuss relevant quality issues that arise – in particular, the need to consider caring as a requirement.

P. Mell, *J. Shook*, R. Harang and *S. Gavrila*. **Linear Time Algorithms to Restrict Insider Access using Multi-Policy Access Control Systems**. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 8(1), pp. 4-25 (March 2017).

https://doi.org/10.22667/JOWUA.2017.03.31.004

An important way to limit malicious insiders from distributing sensitive information is to restrict access as tightly as possible. This has always been the goal in the design of access control mechanisms, but individual approaches can be inadequate. Approaches that instantiate multiple methods simultaneously have been shown to restrict access

with more precision. However, those approaches have had limited scalability (resulting in exponential calculations in some cases).

In this work, we provide an implementation of the Next Generation Access Control (NGAC) standard from the American National Standards Institute (ANSI) and demonstrate that it scales. The existing publicly available reference implementations all use cubic algorithms for policy decisions, and thus, NGAC was widely viewed as not scalable. Our approach provides an easy to understand graph algorithm that performs policy decisions in linear time at the worst. However, in practice, the algorithm runs considerably faster. We also provide a default linear-time mechanism to visualize and review user access rights for an ensemble of access control mechanisms. Our visualization appears to be a simple file directory hierarchy, but in reality is an automatically generated structure abstracted from the underlying access control graph that works with any set of simultaneously instantiated access control policies. It also provides an implicit mechanism for symbolic linking that provides a powerful access capability. Our work has thus lead to the first efficient implementation of NGAC while enabling user privilege review through a novel visualization approach.

C. Miller and Y. Shi. **Randomness in Nonlocal Games Between Mistrustful Players**. *Quantum Information & Computation* 17(7&8), pp. 595-610 (June 2017).

https://doi.org/10.26421/QIC17.7-8

If two quantum players at a nonlocal game G achieve a superclassical score, then their measurement outcomes must be at least partially random from the perspective of any third player. This is the basis for device-independent quantum cryptography. In this paper we address a related question: does a superclassical score at G guarantee that one player has created randomness from the perspective of the other player? We show that for complete-support games, the answer is yes; even if the second player is given the first player's input at the conclusion of the game, he cannot perfectly recover her output. Thus, some amount of *local* randomness (i.e., randomness possessed by only one player) is always obtained when randomness is certified from nonlocal games with quantum strategies. This is in contrast to non-signaling game strategies, which may produce global randomness without any local randomness. We discuss potential implications for cryptographic protocols between mistrustful parties.

D. Moody and A.A. Ciss. **Arithmetic Progressions on Conics**. *Journal of Integer Sequences* 20(1), article no. 17.2.6, pp. 1-8 (December 27, 2016).

https://cs.uwaterloo.ca/journals/JIS/VOL20/Moody/moody7.html

In this paper, we look at long arithmetic progressions on conics. By an arithmetic progression on a curve, we mean the existence of rational points on the curve whose x-coordinates are in arithmetic progression. We revisit arithmetic progressions on the unit circle, constructing 3-term progressions of points in the first quadrant containing an arbitrary rational point on the unit circle. We also provide infinite families of 3-term progressions on the unit hyperbola, as well as conics $ax^2 + cy^2 = 1$ containing arithmetic progressions as long as 8 terms.

D. Simos, *D.R. Kuhn*, *A. Voyiatzis* and *R.N. Kacker*. **Combinatorial Methods in Security Testing**. *Computer (IEEE)* 49(10), pp. 80-83 (October 2016).

https://doi.org/10.1109/MC.2016.314

Combinatorial methods can make software security testing much more efficient and effective than conventional approaches.

J. Torres-Jimenez, I. Izquierdo-Marquez, D. Ramirez-Acuna and *R. Peralta*. **Near-Optimal Algorithm to Count Occurrences of Subsequences of a Given Length**. *Discrete Mathematics, Algorithms and Applications* 9(3), 10 pp. (June 2017).

https://doi.org/10.1142/S1793830917500422

For $k \in \mathbb{Z}^+$, define Σ_k as the set of integers $\{0,1,\ldots, k-1\}$. Given an integer n and a string t of length $m \geq n$ over Σ_k, we count the number of times that each one of the k^n distinct strings of length n over Σ_k occurs as a subsequence of t. Our algorithm makes only one scan of t and solves the problem in time complexity mk^{n-1} and space complexity $m+k^n$. These are very close to best possible results.

J. Voas and *D.R. Kuhn*. **What Happened to Software Metrics?** *Computer (IEEE Computer)* 50(5), pp. 88-98 (May 2017).

https://doi.org/10.1109/MC.2017.144

In the 1980's, the software quality community was all "a buzz" with seemingly endless "potential" approaches for producing higher quality software. At the forefront of that was software metrics, along with the corresponding software testing techniques and tools and process improvement schemes that relied on the software metrics. We asked a panel of 7 software metrics experts 11 questions to help explain the last 40 years of software measurement and where they believe we stand today. Our experts are: (1) Taghi Khoshgoftaar (Florida Atlantic University), (2) Edward F. Miller (Software Research, Inc.), (3) Vic Basili (University of Maryland, retired), (4) Jim Bieman (Colorado State University), (5) Ram Chillarege (Chillarege, Inc.), (6) Adam Porter (Fraunhofer Institute), and (7) Alain Abran (University of Québec). We did not ask rhetorical questions, but rather questions that we believe remain unanswered, and if answered, could form a foundation for improved or new software metrics and software measurement.

CONFERENCE PAPERS

N. Alhebaishi, L. Wang, S. Jajodia and *A. Singhal*. **Threat Modeling for Cloud Data Center Infrastructures**. *9th International Symposium on Foundations and Practice of Security (FPS 2016)*, Québec City, Québec, Canada, October 24-26, 2016. In *Lecture Notes in Computer Science* 10128, *Foundations and Practice of Security (Revised Selected Papers)*, pp. 302-319.

https://doi.org/10.1007/978-3-319-51966-1_20

Cloud computing has undergone rapid expansion throughout the last decade. Many companies and organizations have made the transition from traditional data centers to the cloud due to its flexibility and lower cost. However, traditional data centers are still being relied upon by those who are less certain about the security of cloud computing. This problem is highlighted by the fact that there only exist limited efforts on threat modeling for cloud data centers. In this paper, we conduct comprehensive threat modeling exercises based on two representative cloud infrastructures using several popular threat modeling methods, including attack surface, attack trees, attack graphs, and security metrics based on attack trees and attack graphs, respectively. Those threat modeling efforts provide cloud providers with practical lessons and the means toward better evaluating, understanding, and improving their cloud infrastructures. Our results may also improve confidence in potential cloud tenants by providing them a clearer picture about potential threats in cloud infrastructures and corresponding solutions.

D. Borbor, L. Wang, S. Jajodia and *A. Singhal*. **Securing Networks Against Unpatchable and Unknown Vulnerabilities Using Heterogeneous Hardening Options**. *31st IFIP Annual Conference on Data and Applications Security and Privacy (DBSEC 2017)*, Philadelphia, Pennsylvania, July 19-21, 2017. In *Lecture Notes in Computer Science* 10359, *DBSec 2017: Data and Applications Security and Privacy XXXI*, pp. 509-528.

https://doi.org/10.1007/978-3-319-61176-1_28

The administrators of a mission critical network usually have to worry about non-traditional threats, e.g., how to live with known, but unpatchable vulnerabilities, and how to improve the network's resilience against potentially unknown vulnerabilities. To this end, network hardening is a well-known preventive security solution that aims to improve network security by taking proactive actions, namely, hardening options. However, most existing network hardening approaches rely on a single hardening option, such as disabling unnecessary services, which becomes less effective when it comes to dealing with unknown and unpatchable vulnerabilities. A heterogeneous approach is lacking that can combine different hardening options in an optimal way to deal with both unknown and unpatchable vulnerabilities. In this paper, we propose such an approach by unifying multiple hardening options, such as firewall rule modification, disabling services, service diversification, and access control, under the same model. We then apply security metrics designed for evaluating network resilience against unknown and unpatchable vulnerabilities, and consequently

derive optimal hardening solutions that maximize security under given cost constraints.

D. Ferraiolo, *S. Gavrila*, *G. Katwala* and *J. Roberts.* **Imposing Fine-grain Next Generation Access Control over Database Queries**. *Proceedings of the 2nd ACM Workshop on Attribute Based Access Control (ABAC '17)*, Scottsdale, Arizona, March 24, 2017, pp. 9-15.

https://doi.org/10.1145/3041048.3041050

In this paper, we describe a system that leverages the ANSI/INCITS Next Generation Access Control (NGAC) standard, called Next-generation Database Access Control (NDAC), for accessing data in tables, rows, and columns in existing Relational Database Management System (RDBMS) products. NDAC imposes access control at the data level, eliminating the need for implementing and managing access control in applications and/or through the use of proprietary RDBMS mechanisms. Consequently, the same policies can protect multiple databases from queries sent from multiple applications. Furthermore, NDAC not only provides control down to the field level, but to varying fields of select rows. NDAC is unique in achieving this granularity of control without the use and coordination of multiple protection mechanisms. Operationally, users issue wide sweeping queries, and NDAC allows access to the optimal amount of data permissible for the user. The method includes an Access Manager for trapping and enforcing policy over the SQL queries issued by applications, as well as a Translator for converting SQL statements to NGAC inputs and converting NGAC authorization responses to either an access deny or one or more permitted SQL statements.

M. Find, A. Golovnev, E.A. Hirsch and A.S. Kulikov. **A Better-Than-3n Lower Bound for the Circuit Complexity of an Explicit Function**. *Proceedings. 57th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2016),* New Brunswick, New Jersey, October 9-11, 2016, pp. 89-98.

https://doi.org/10.1109/FOCS.2016.19

We consider Boolean circuits over the full binary basis. We prove a (3+1/86)*n*-o(*n*) lower bound on the size of such a circuit for an explicitly defined predicate, namely an affine disperser for sublinear dimension. This improves the 3*n*-o(*n*) bound of Norbert Blum (1984). The proof is based on the gate elimination technique extended with the following three ideas. We generalize the computational model by allowing circuits to contain cycles; this in turn allows us to perform affine substitutions. We use a carefully chosen circuit complexity measure to track the progress of the gate elimination process. Finally, we use quadratic substitutions that may be viewed as delayed affine substitutions.

Y. Hanatani, N. Ogura, Y. Ohba, *L. Chen* and S. Das. **Secure Multicast Group Management and Key Distribution in IEEE 802.21**. *3rd International Conference on Research in Security Standardisation (SSR 2016)*, Gaithersburg, Maryland, December 5-6, 2016. In *Lecture Notes in Computer Science* 10074, *Security Standardisation Research. SSR 2016*, pp. 227-243.

https://doi.org/10.1007/978-3-319-49100-4_10

Controlling a large number of devices such as sensors and smart end points is always a challenge where scalability and security are indispensable. This is even more important when it comes to periodic configuration updates to a large number of such devices belonging to one or more groups. One solution could be to take a group of devices as a unit of control and then manage them through a group communication mechanism. An obvious challenge to this approach is how to create such groups dynamically and manage them securely. Moreover, there need to be mechanisms in place by which members of the group can be removed and added dynamically.

In this paper, we propose a technique that has been recently standardized in IEEE 802.21 (IEEE Std 802.21d™-2015) with the objective of providing a standard-based solution to the above challenges. The approach relies on the Logical Key Hierarchy (LKH) based key distribution mechanism, but optimizes the number of encryption and decryption operations by using a "Complete Subtree". It leverages the IEEE 802.21 framework, services, and protocol for communication and management, and provides a scalable and secure way to manage (e.g., add and remove) devices from one or more groups. We describe the group key distribution protocol

in detail and provide a security analysis of the scheme along with some performance results from a prototype implementation.

R. Harang and *P. Mell*. **Micro-Signatures: The Effectiveness of Known Bad N-Grams for Network Anomaly Detection**. *9th International Symposium on Foundations and Practice of Security*, Québec City, Québec, Canada, October 24-26, 2016. In *Lecture Notes in Computer Science* 10128, *Foundations and Practice of Security (Revised Selected Papers)*, pp. 36-47.

https://doi.org/10.1007/978-3-319-51966-1_3

Network intrusion detection is broadly divided into signature and anomaly detection. The former identifies patterns associated with known attacks, and the latter attempts to learn a "normal" pattern of activity and provides an alert when behaviors outside of those norms is detected. The *n*-gram methodology has arguably been the most successful technique for network anomaly detection. In this work, we discovered that when training data is sanitized, *n*-gram anomaly detection is not primarily anomaly detection, as it receives the majority of its performance from an implicit non-anomaly subsystem that neither uses typical signatures nor is anomaly-based (though it is closely related to both). We find that for our data, these "micro-signatures" provide the vast majority of the detection capability. This finding changes how we understand and approach *n*-gram based 'anomaly' detection. By understanding the foundational principles upon which it operates, we can then better explore how to optimally improve it.

J. Jones, T. Khan, K. Laskey, *A. Nelson*, *M. Laamanen* and *D. White*. **Inferring Previously Uninstalled Applications from Digital Traces**. *Proceedings of the 11th Annual Conference on Digital Forensics, Security and Law (ADFSL)*, Daytona Beach, Florida, May 24-26, 2017, pp. 113-130.

http://commons.erau.edu/adfsl/2016/wednesday/3/

In this paper, we present an approach and experimental results to suggest the past presence of an application after the application has been uninstalled and the system has remained in use. Current techniques rely on the recovery of intact artifacts and traces, e.g., whole files, Windows Registry entries, or log file entries, while our approach requires no intact artifact recovery and leverages trace evidence in the form of residual partial files. In the case of recently uninstalled applications or an instrumented infrastructure, artifacts and traces may be intact and complete. In most cases, however, digital artifacts and traces are altered, destroyed, and disassociated over time, due to normal system operation and deliberate obfuscation activity. As a result, analysts are often presented with partial and incomplete artifacts and traces from which defensible conclusions must be drawn.

In this work, we match the sectors from a hard disk of interest to a previously constructed catalog of full files captured while various applications were installed, used, and uninstalled. The sectors composing the files in the catalog are not necessarily unique to each file or application, so we use an inverse frequency-weighting scheme to compute the inferential value of matched sectors. Similarly, we compute the fraction of full files associated with each application that is matched, where each file with a sector match is weighted by the fraction of total catalog sectors matched for that file. We compared results using both the sector-weighted and file-weighted values for known ground truth-test images and final-snapshot images from the M57 Patents Scenario data set. The file-weighted measure was slightly more accurate than the sector-weighted measure, although both identified all of the uninstalled applications in the test images and a high percentage of installed and uninstalled applications in the M57 data set, with minimal false positives for both sets.

The key contribution of our work is the suggestion of uninstalled applications through weighted measurement of residual file fragments. Our experimental results indicate that past application activity can be reliably indicated even after an application has been uninstalled, and the host system has been rebooted and used. The rapid and reliable indication of previously uninstalled applications is useful for cyber defense, law enforcement, and intelligence operations.

L. Khati, *N. Mouha* and D. Vergnaud. **Full Disk Encryption: Bridging Theory and Practice**. *RSA Conference 2017*, San Francisco, California, February

14-17, 2017. In *Lecture Notes in Computer Science* 10159, *Topics in Cryptology – CT-RSA 2017*, pp. 241-257.

https://doi.org/10.1007/978-3-319-52153-4_14

We revisit the problem of Full Disk Encryption (FDE), which refers to the encryption of each sector of a disk volume. In the context of FDE, it is assumed that there is no space to store additional data, such as an IV (Initialization Vector) or a MAC (Message Authentication Code) value. We formally define the security notions in this model against chosen-plaintext and chosen-ciphertext attacks. Then, we classify various FDE modes of operation according to their security in this setting, in the presence of various restrictions on the queries of the adversary. We found that our approach leads to new insights for both theory and practice. Moreover, we introduce the notion of a diversifier, which does not require additional storage, but allows the plaintext of a particular sector to be encrypted to different ciphertexts. We show how a 2-bit diversifier can be implemented in the EagleTree simulator for solid state drives (SSDs), while decreasing the total number of Input/Output Operations Per Second (IOPS) by only 4 %.

D.R. Kuhn, M. Raunak and *R.N. Kacker*. **An Analysis of Vulnerability Trends, 2008-2016**. *Proceedings. 2017 IEEE International Conference on Software Quality, Reliability and Security (Companion Volume) (QRS-C 2017)*, Prague, Czech Republic, July 25-29, 2017, pp. 587-588.

https://doi.org/10.1109/QRS-C.2017.106

Computer security has been a subject of serious study for at least 40 years, and a steady stream of innovations has improved our ability to protect networks and applications. But attackers have adapted and changed methods over the years as well. Where do we stand today in the battle between attackers and defenders? Are attackers gaining ground, as it often seems when reading press accounts of the latest data exposure? This analysis seeks to answer these questions using data from the U.S. National Vulnerability Database (NVD), and to identify classes of vulnerabilities where improvements will be most cost effective.

C. Liu, *A. Singhal* and D. Wijesekera. **Identifying Evidence for Cloud Forensic Analysis**. *IFIP WG 11.3 International Conference on Digital Forensics*, Orlando, Florida, January 30 – February 1, 2017. In *IFIP Advances in Information and Communication Technology* 511, *Advances in Digital Forensics XIII, Revised Selected Papers*, pp. 111-130.

https://doi.org/10.1007/978-3-319-67208-3_7

Cloud computing provides benefits such as increased flexibility, scalability and cost savings to enterprises. However, it introduces several challenges to digital forensic investigations. Current forensic analysis frameworks and tools are largely intended for offline investigations, and it is assumed that the logs are under investigator control. In cloud computing, however, evidence can be distributed across several machines, most of which would be outside the control of the investigator. Other challenges include the dependence of forensically valuable data on the cloud deployment model, large volumes of data, proprietary data formats, multiple isolated virtual machine instances running on a single physical machine and inadequate tools for conducting cloud forensic investigations.

This research demonstrates that evidence from multiple sources can be used to reconstruct cloud attack scenarios. The sources include: (i) intrusion detection system and application software logs; (ii) cloud service API calls; and (iii) system calls from virtual machines. A forensic analysis framework for cloud computing environments is presented that considers logged data related to activities in the application layer as well as lower layers. A Prolog-based forensic analysis tool is used to automate the correlation of evidence from clients and the cloud service provider in order to reconstruct attack scenarios in a forensic investigation.

P. Mell, *S. Gavrila* and *J. Shook*. **Restricting Insider Access through Efficient Implementation of Multi-Policy Access Control Systems**. *MIST '16: Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats*, Vienna, Austria, October 24-28, 2016, pp. 13-22.

https://doi.org/10.1145/2995959.2995961

The American National Standards Organization has standardized an access control approach, Next Generation Access Control (NGAC), that enables the simultaneous instantiation of multiple access

control policies. For large complex enterprises, this is critical to limiting the legally authorized access by insiders. However, the specifications describe the required access control capabilities but not the related algorithms. Existing reference implementations have inefficient algorithms and thus, do not fully express the NGAC's ability to scale.

For example, the primary NGAC reference implementation took several minutes to simply display the set of files accessible to a user on a moderately sized system. To solve this problem, we provide efficient algorithms, reducing the overall complexity from cubic to quadratic. Our other major contribution is to provide a novel mechanism for administrators and users to review allowed access rights. We provide an interface that appears to be a simple file directory hierarchy but in reality is an automatically generated structure abstracted from the underlying access control graph that works with any set of simultaneously instantiated access control policies. Our work thus provides the first efficient implementation of NGAC while enabling user privilege review through a novel visualization approach. It thereby enables the efficient simultaneous instantiation of multiple access control policies that is needed to best limit insider access to information (and thereby limit information leakage).

P. Mell, *J. Shook* and R. Harang. **Measuring and Improving the Effectiveness of Defense-in-Depth Postures**. *Proceedings of the 2nd Annual Industrial Control System Security Workshop (ICSS '16)*, Los Angeles, California, December 6, 2016, pp. 15-22.

https://doi.org/10.1145/3018981.3018986

Defense-in-depth is an important security architecture principle that has significant application to industrial control systems (ICS), cloud services, storehouses of sensitive data, and many other areas. We claim that an ideal defense-in-depth posture is "deep," containing many layers of security, and "narrow," the number of node independent attack paths is minimized. Unfortunately, accurately calculating both depth and width is difficult using standard graph algorithms because of a lack of independence between multiple vulnerability instances (i.e., if an attacker can penetrate a particular vulnerability on one host, then they can likely penetrate the same vulnerability on another host). To address this, we represent known weaknesses and vulnerabilities as a type of colored attack graph. We measure depth and width through solving the shortest color path and minimum color cut problems. We prove both of these to be NP-Hard and thus, for our solution, we provide a suite of greedy heuristics. We then empirically apply our approach to large randomly generated networks as well as to ICS networks generated from a published ICS attack template. Lastly, we discuss how to use these results to help guide improvements to defense-in-depth postures.

D. Moody, *R. Perlner* and *D. Smith-Tone*. **Improved Attacks for Characteristic-2 Parameters of the Cubic ABC Simple Matrix Encryption Scheme**. *8th International Workshop on Post-Quantum Cryptography (PQCrypto 2017)*, Utrecht, The Netherlands, June 26-28, 2017. In *Lecture Notes in Computer Science* 10346, *Post-Quantum Cryptography - PQCrypto 2017*, pp. 255-271.

https://doi.org/10.1007/978-3-319-59879-6_15

In the last few years multivariate public key cryptography has experienced an infusion of new ideas for encryption. Among these new strategies is the ABC Simple Matrix family of encryption schemes that utilize the structure of a large matrix algebra to construct effectively invertible systems of nonlinear equations hidden by an isomorphism of polynomials. One promising approach to cryptanalyzing these schemes has been structural cryptanalysis, based on applying a strategy similar to MinRank attacks to the discrete differential. These attacks however have been significantly more expensive when applied to parameters using fields of characteristic 2, which have been the most common choice for published parameters. This disparity is especially great for the cubic version of the Simple Matrix Encryption Scheme.

In this work, we demonstrate a technique that can be used to implement a structural attack that is as efficient against parameters of characteristic 2 as are attacks against analogous parameters over higher characteristic fields. This attack demonstrates that, not only is the cubic simple matrix scheme susceptible to structural attacks, but that the published parameters claiming 80 bits of security are less secure than claimed (albeit only slightly.)

Similar techniques can also be applied to improve structural attacks against the original Simple Matrix Encryption scheme, but they represent only a modest improvement over previous structural attacks. This work therefore demonstrates that choosing a field of characteristic 2 for the Simple Matrix Encryption Scheme or its cubic variant will not provide any additional security value.

A. Petzoldt, M.-S. Chen, J. Ding and B.-Y. Yang. **HMFEv - An Efficient Multivariate Signature Scheme**. *8th International Workshop on Post-Quantum Cryptography (PQCrypto 2017)*, Utrecht, The Netherlands, June 26-28, 2017. In *Lecture Notes in Computer Science* 10346, *Post-Quantum Cryptography - PQCrypto 2017*, pp. 205-223.

https://doi.org/10.1007/978-3-319-59879-6_12

Multivariate Cryptography, as one of the main candidates for establishing post-quantum cryptosystems, provides strong, efficient and well-understood digital signature schemes such as Unbalanced Oil-Vinegar (UOV), Rainbow, and Gui. While Gui provides very short signatures, it is, for efficiency reasons, restricted to very small finite fields, which makes it hard to scale it to higher levels of security and leads to large key sizes.

In this paper we propose a signature scheme called HMFEv ("Hidden Medium Field Equations"), which can be seen as a multivariate version of HFEv ("Hidden Field Equation"). We obtain our scheme by applying the Vinegar Variation to the Multi-HFE encryption scheme of Chen et al. We show both theoretically and by experiments that our new scheme is secure against direct and Rank attacks. In contrast to other schemes of the HFE family such as Gui, HMFEv can be defined over arbitrary base fields and therefore is much more efficient in terms of both performance and memory requirements. Our scheme is therefore a good candidate for the upcoming standardization of post-quantum signature schemes.

M. Raunak, *D.R. Kuhn* and *R.N. Kacker*. **Combinatorial Testing of Full Text Search in Web Applications**. *Proceedings. 2017 IEEE International Conference on Software Quality, Reliability and Security (Companion Volume) (QRS-C 2017)*, Prague, Czech Republic, July 25-29, 2017, pp. 100-107.

https://doi.org/10.1109/QRS-C.2017.24

Database-driven web applications are some of the most widely developed systems today. In this paper, we demonstrate the use of combinatorial testing for testing database-supported web applications, especially where full-text search is provided or many combinations of search options are utilized. We develop test-case selection techniques, where test strings are synthesized using characters or string fragments that may lead to system failure. We have applied our approach to the National Vulnerability Database (NVD) application and have discovered a number of "corner-cases" that had not been identified previously. We also present simple heuristics for isolating the fault-causing factors that can lead to such system failures. The test method and input model described in this paper have immediate application to other systems that provide complex full text search.

X. Sun, *A. Singhal* and P. Liu. **Towards Actionable Mission Impact Assessment in the Context of Cloud Computing**. *31st IFIP Annual Conference on Data and Applications Security and Privacy (DBSEC 2017)*, Philadelphia, Pennsylvania, July 19-21, 2017. In *Lecture Notes in Computer Science* 10359, *DBSec 2017: Data and Applications Security and Privacy XXXI*, pp. 259-274.

https://doi.org/10.1007/978-3-319-61176-1_14

Today's cyber-attacks toward enterprise networks often undermine and even fail the mission assurance of victim networks. Mission cyber resilience (or active cyber defense) is critical to prevent or minimize the negative consequences that would impact missions. Without effective mission impact assessment, mission cyber resilience cannot be really achieved. However, there is an overlooked gap between mission impact assessment and cyber resilience due to the non-mission-centric nature of current research. This gap is even widened in the context of cloud computing. The gap essentially accounts for the weakest link between missions and attack-resilient systems, and also explains why the existing impact analysis is not really actionable.

This paper initiates efforts to bridge this gap by developing a novel graphical model that interconnects the mission dependency graphs and

cloud-level attack graphs. Our case study shows that the new cloud-applicable model is able to bridge the gap between mission impact assessment and cyber resilience. As a result, it can significantly improve the effectiveness of the cyber resilience analysis of mission critical systems.

S. Vilkomir, A. Alluri, *D.R. Kuhn* and *R.N. Kacker*. **Combinatorial and MC/DC Coverage Levels of Random Testing**. *2017 IEEE International Conference on Software Quality Reliability and Security (QRS-C 2017)*, Prague, Czech Republic, July 25-29, 2017, pp. 61-68.

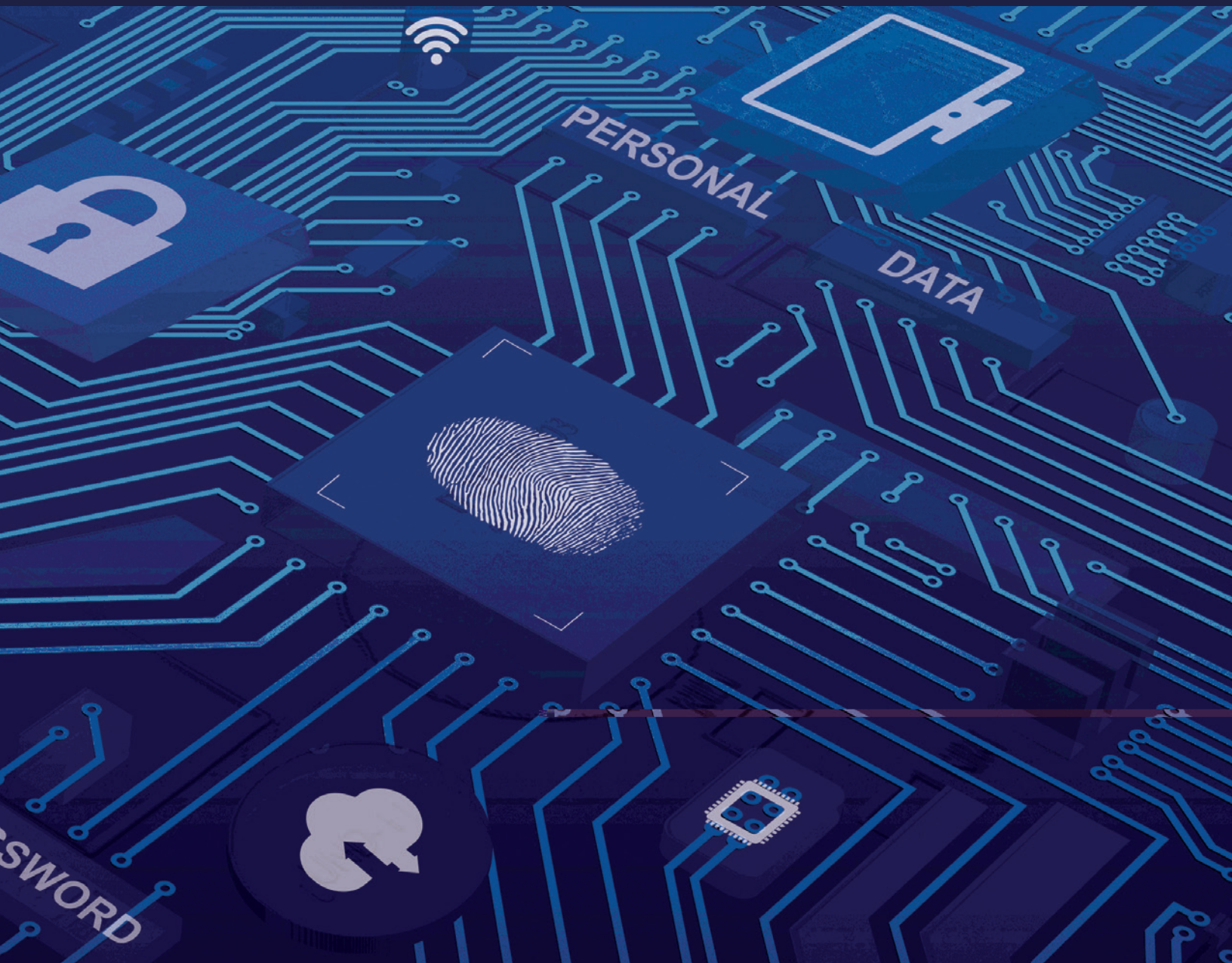
https://doi.org/10.1109/QRS-C.2017.19

Software testing criteria differ in their effectiveness, the numbers of test cases required, and the processes of test generation. Specific criteria often are compared to random testing, and in some cases, random testing shows a surprisingly high level of effectiveness. One reason that this is the case is that any random test set has a specific level of coverage according to any coverage criterion. The numerical evaluation of coverage levels of random testing according to various coverage criteria is an interesting research task and is important in understanding the relationship between different testing approaches.

In this paper, we performed an experimental evaluation of the coverage levels of random testing for two criteria: Modified Condition/Decision Coverage (MC/DC) and combinatorial t-way testing. Our experiments showed that, when the number of random test cases increased, a high level of coverage was reached rapidly, both for MC/DC and t-way. However, many more random tests are required to reach 100 % coverage. An unexpected result was that there were significant differences in the measurement of partial MC/DC coverage by various tools. The results may be used to select optimal methods for practical testing and develop new testing methods based on the integration of existing approaches.

APPENDICES

The next section contains 3 Appendices (List of Acronyms, NIST/ITL Cybersecurity Events, and Ways to Engage with ITL Cybersecurity Program and NIST).



APPENDIX A: ACRONYMS

3GPP	3rd Generation Partnership Project
4G	4th Generation
5G	5th Generation
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
ADFSL	Annual Conference on Digital Forensics, Security and Law
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AIM	Algorithms for Intrusion Measurement
AN-ITL	ANSI/NIST-ITL
ANS	American National Standard
ANSI	American National Standards Institute
ANTD	Advanced Network Technologies Division
API	Application Programming Interface
ARF	Asset Reporting Format
ARM	Access Rights Management
ARM	(also) Advanced Reduced Instruction Set Computing (RISC) Machine
AS	Autonomous System
ASKDF	Application-Specific Key Derivation Functions
BF	Bugs Framework
BGP	Border Gateway Protocol
BioCTS	Biometric Conformance Test Software
BIOS	Basic Input/Output System
BOF	Buffer Overflow
CASSA	Cognitive-based Approach to System Security Assessment
CAVP	Cryptographic Algorithm Validation Program
CBC	CipherBlock Chaining
CBOR	Concise Binary Object Representation
CCE	Common Configuration Enumeration
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CCSS	Common Configuration Scoring System
CDH	Co-factor Diffie-Hellman
CDM	Continuous Diagnostics and Mitigation
CFReDS	Computer Forensics Reference Data Sets
CFTT	Computer Forensic Tool Testing
CIF	Control of Interaction Frequency
CIO	Chief Information Officer
CIS	Center for Internet Security

CLI	Command Line Interface
CMAC	Cipher-based Message Authentication Code
CMUF	Cryptographic Modules User Forum
CMVP	Cryptographic Module Validation Program
CNSS	Committee on National Security Systems
CNSSD	CNSS Directive
CoP	Community of Practice
CPE	Common Platform Enumeration
CPS	Cyber-Physical Systems
CRADA	Cooperative Research and Development Agreement
CREDC	Cyber Resilient Energy Delivery Consortium
C-SCRM	Cyber Supply Chain Risk Management
CSD	Computer Security Division
CSE	Communications Security Establishment
CSF	Cybersecurity Framework
CSIA	Cybersecurity and Information Assurance
CSP	Credential Service Provider
CSRC	Cloud Security Rubik's Cube
CSRC	(also) Computer Security Resource Center
CSSPAB	Computer System Security and Privacy Advisory Board
CST	Cryptographic and Security Testing
CTG	Cryptographic Technology Group
CTM	Conformance Testing Methodology
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
CVP	Cryptographic Validation Program
CVSS	Common Vulnerability Scoring System
CVSS-SIG	CVSS Special Interest Group
CWI	Centrum Wiskunde & Informatica
DARPA	Defense Advanced Research Project Agency
DDoS	Distributed Denial of Service
DEA	Data Encryption Algorithm
DH	Diffie-Hellman
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DKIM	Domain Keys Identified Mail
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoD	Department of Defense
DoE	Department of Energy
DPC	Derived PIV Credentials
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard

DTR	Derived Test Requirements
EaaS	Entropy as a Service
ECC	Elliptic Curve Cryptography
ECP	Enterprise Compliance Profile
EDR	Enhanced Data Rate
EISA	Energy Independence and Security Act
EL	Engineering Laboratory
EM	Encoded Message
EO	Executive Order
ESDC	Employment and Social Development Canada
ETSI	European Telecommunication Standardisation Institute
FAQ	Frequently Asked Questions
FAR	Federal Acquisition Regulation
FASTER	Faster Administration of S&T Education and Research
FCSM	Federal Computer Security Managers
FDCC	Federal Desktop Core Configuration
FDE	Full Disk Encryption
FEMA	Federal Emergency Management Agency
FFRDC	Federally Funded Research and Development Center
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
FOP	Faulty Operation
FPE	Format-Preserving Encryption
FY	Fiscal Year
GAO	Government Accountability Office
GCM	Galois/Counter Mode
GCSE	Group Communication System Enablers
GMAC	Galois Message Authentication Code
GSA	General Services Administration
GUI	Graphical User Interface
HAVA	Help America Vote Act
HDO	Healthcare Delivery Organization
HFEv	Hidden Field Equation
HHS	Health and Human Services
HIMSS	Healthcare Information and Management Systems Society
HIPAA	Health Insurance Portability and Accountability Act
HMAC	Hash-based Message Authentication Code
HMFEv	Hidden Medium Field Equation
HS	High Speed
HSPD-12	Homeland Security Presidential Directive-12
HTML5	Hypertext Markup Language version 5

HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
HWAM	Hardware Asset Management
IAD	Information Access Division
IARPA	Intelligence Advanced Research Projects Activity
IC	Intelligence Community
ICMC	International Cryptographic Module Conference
ICS	Industrial Control Systems
ICSP	Interagency Council on Standards Policy
IdAM	Identity and Access Management
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
IICS WG	Interagency International Cybersecurity Standardization Working Group
IIP	Internet Infrastructure Protection
IKE	Internet Key Exchange
INCITS	InterNational Committee for Information Technology Standards
INFORMS	Institute for Operations Research and the Management Sciences
INJ	Injection
I/O	Input/Output
IOPS	Input/Output Operations Per Second
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
IRS	Internal Revenue Service
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
ISP	Internet Service Provider
ISPAB	Information Security and Privacy Advisory Board
IT	Information Technology
ITL	Information Technology Laboratory
IUT	Implementation Under Test
IV	Initialization Vector
IVA	Intelligent Virtual Assistant
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

KMN	Key Management
KSAs	Knowledge, Skills, and Abilities
LKH	Logical Key Hierarchy
LTE	Long Term Evolution
MAC	Message Authentication Code
MAL	Memory Allocation
MC/DC	Modified Condition/Decision Coverage
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
NARA	National Archives and Records Administration
NCCIC	National Cybersecurity and Communications Integration Center
NCCoE	National Cybersecurity Center of Excellence
NCP	National Checklist Program
NCSA	National Cyber Security Alliance
NDAC	Next-generation Database Access Control
NEA	Network Endpoint Assessment
NGAC	Next Generation Access Control
NGAC-GOADS	Next Generation Access Control – Generic Operations & Abstract Data Structures
NGAC-IRPADS	Next Generation Access Control-Implementation Requirements, Protocols and API Definitions
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NICE	National Initiative for Cybersecurity Education
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
NREL	National Renewable Energy Laboratory
NSA	National Security Agency
NSRL	National Software Reference Library
NTIA	National Telecommunications and Information Administration
NVD	National Vulnerability Database
NVLAP	National Voluntary Laboratory Accreditation Program
OASIS	Organization for the Advancement of Structured Information Standards

OCIL	Open Checklist Interactive Language
OEMs	Original Equipment Manufacturers
OISM	Office of Information Systems Management
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OS	Operating System
OSCAL	Open Security Controls Assessment Language
OSHE	Office of Safety, Health and Environment
OVAL	Open Vulnerability and Assessment Language
PCI	Payment Card Industry
DSS PCI	Data Security Standard Payment Card Industry
PEP	Privacy Engineering Program
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
P.L.	Public Law
PM	Policy Machine
PML	Physical Measurement Laboratory
PMS	Property Management Systems
POS	Point-of-Sale
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
R&D	Research and Development
RAM	Random Access Memory
RBAC	Role-Based Access Control
RBG	Random Bit Generator
RDBMS	Relational Database Management System
RDS	Reference Data Set
RFC	Request for Comments
RIDR	Robust Inter-Domain Routing
RISC	Reduced Instruction Set Computing
RMF	Risk Management Framework
RNG	Random Number Generation
ROA	Route Origin Authorization
ROLIE	Resource-Oriented Lightweight Information Exchange
ROV	Route Origin Validation
RPs	Relying Parties
RPKI	Resource Public Key Infrastructure
RSA	Rivest, Shamir, Adleman
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
SCAP	Security Content Automation Protocol
SCAPVal	SCAP Content Validation Tool
SCORE	Special Cyber Operations Research and Engineering
SCRM	Supply Chain Risk Management
SDO	Standards Developing Organizations
SEPA	Smart Electric Power Alliance
SGCC	Smart Grid Cybersecurity Committee
SGIP	Smart Grid Interoperability Panel
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SIDR	Secure Inter-Domain Routing
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
SOFA-B	Strength of Function for Authenticators – Biometrics
SP	Special Publications
SPF	Sender Policy Framework
SRAM	Static Random Access Memory
SSCA	Software and Supply Chain Assurance
SSD	Software and Systems Division
SSDs	Solid State Drives
SSH	Secure Shell
SSLF	Specialized Security-Limited Functionality
SSO	Single Sign-on
SSP	System Security Plan
STIG	Security Technical Implementation Guide
STVMG	Security Testing, Validation, and Measurement Group
SWID	Software Identification
SWIMA	Software Inventory Message and Attributes
SwMM-RSV	Software Measures and Metrics to Reduce Security Vulnerabilities
TC	Technical Committee
TCB	Trusted Computing Base
TCG	Trusted Computing Group
TCI	Toolchain Infrastructure
TDEA	Triple Data Encryption Algorithm
TDES	Triple Data Encryption Standard
TIG	Trusted Identities Group
TLS	Transport Layer Security
TMSAD	Trust Model for Security Automation Data
TNC	Trusted Network Connect
TPM	Trusted Platform Module
TTPs	Tactics, Techniques, and Procedures

UOV	Unbalanced Oil-Vinegar Digital Signature Scheme
URL	Uniform Resource Locator
US-CERT	U.S. Computer Emergency Readiness Team
USG	U.S. Government
VM	Virtual Machine
VPN	Virtual Private Network
VRDX-SIG	Vulnerability Reporting and Data eXchange SIG
VRF	Verification
W3C	World Wide Web Consortium
WG	Working Group
WPANs	Wireless Personal Area Networks
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 2017

The list below describes numerous events hosted and/or supported by the ITL Cybersecurity Program. Please note that the list does not include all the events at which the NIST staff presented.

SEPTEMBER 2017

NICE Webinar: Efforts to Align Training and Certifications to the NICE Framework
September 20
Webinar
https://www.nist.gov/news-events/events/2017/09/nice-webinar-efforts-align-training-and-certifications-nice-framework

NCCoE National Cybersecurity Excellence Partnership In-Person Meeting @ Juniper Networks
September 14
Sunnyvale, California

Safeguarding Health Information: Building Assurance through HIPAA Security – 2017
September 5-6
Washington D.C.
https://www.nist.gov/news-events/events/2017/09/safeguarding-health-information-building-assurance-through-hipaa-security

AUGUST 2017

Summer 2017 Software and Supply Chain Assurance Forum
August 29-30
McLean, Virginia
https://csrc.nist.gov/Events/2017/Summer-2017-Software-and-Supply-Chain-Assurance-Fo

Medical Device Cybersecurity & Interoperability Workshop
August 29, 2017
Rockville, MD
https://content.govdelivery.com/attachments/USNIST/2017/08/25/file_attachments/869093/Federal%2BCollaboration%2BEnvironment%2BFramwork%2B20170823.pdf

Federal Computer Security Program Managers' Forum Meeting
August 16
NIST Gaithersburg, MD.
https://csrc.nist.gov/Events/2017/Federal-Computer-Security-Managers-Forum-Meeting

Workshop on Cybersecurity Workforce Development
August 2
Chicago, Illinois
https://www.nist.gov/news-events/events/2017/08/workshop-cybersecurity-workforce-development

JULY 2017

Universal CPS Environment for Federation Workshop
July 27
NCCoE Facility (NIST) Rockville, MD.
https://www.nist.gov/news-events/events/2017/07/universal-cps-environment-federation-workshop

NICE Webinar: Shedding Light on Security Clearances - Process, Requirements, and Considerations
July 19
Webinar
https://www.nist.gov/news-events/events/2017/07/nice-webinar-shedding-light-security-clearances-process-requirements-and

Enhancing Resiliencxwe of the Internet and Communications Ecosystem
July 11-12
NIST Gaithersburg, MD.
https://www.nist.gov/news-events/events/2017/07/enhancing-resilience-internet-and-communications-ecosystem

JUNE 2017

ISPAB Meeting
June 28-30
Washington D.C.
https://csrc.nist.gov/Events/2017/ISPAB-June-2017-Meeting

NICE Webinar: Positioning the National Guard to Augment the Cybersecurity Workforce
June 21
Webinar
https://www.nist.gov/news-events/events/2017/06/nice-webinar-positioning-national-guard-augment-cybersecurity-workforce

Federal Computer Security Managers' Forum - 2 day Annual Offsite Meeting
June 20-21
NIST Gaithersburg, MD.
https://csrc.nist.gov/Events/2017/Federal-Computer-Security-Managers-Forum-2-day

Federal Information Systems Security Educators' Association (FISSEA) 30th Annual Meeting
June 19
NIST Gaithersburg, MD.
https://www.nist.gov/news-events/events/2017/06/federal-information-systems-security-educators-association-fissea-30th

2017 PSCR Public Safety Broadband Stakeholder Meeting
June 12-14
NIST Gaithersburg, MD.
https://www.nist.gov/news-events/events/2017/06/2017-pscr-public-safety-broadband-stakeholder-meeting

National Cyber Summit
June 6-8
Huntsville, Alabama
https://www.nist.gov/news-events/events/2017/06/national-cyber-summit-huntsville-alabama

The President's Executive Order on Cybersecurity Workforce: Next Steps and How to Engage
June 5
Webinar
https://www.nist.gov/news-events/events/2017/06/presidents-executive-order-cybersecurity-workforce-next-steps-and-how

Privacy Risk Assessment: A Prerequisite for Privacy Risk Management
June 5
NIST Gaithersburg, MD.
https://www.nist.gov/news-events/events/2017/06/privacy-risk-assessment-prerequisite-privacy-risk-management

MAY 2017

SATE VI Organizing Meeting
May 31
NIST Gaithersburg, MD.
https://www.nist.gov/video/webinar-static-analysis-tool-exposition-sate-vi

https://www.nist.gov/news-events/events/2017/05/sixth-static-analysis-tool-exposition-sate-vi

NCCoE Speaker Series: Continuous Diagnostics and Mitigation
May 17
Rockville, MD
https://nccoe.nist.gov/events/nccoe-speaker-series-continuous-diagnostics-and-mitigation

Cybersecurity Framework Workshop 2017
May 16-17
NIST Gaithersburg, MD.
https://www.nist.gov/news-events/events/2017/05/cybersecurity-framework-workshop-2017

NCCoE Speaker Series: Improving the Customer Experience Without Increasing Cyber Risk - A Hospitality Challenge
May 3
Rockville, MD
https://nccoe.nist.gov/events/improving-customer-experience-without-increasing-cyber-risk-hospitality-challenge

APRIL 2017

NICE Webinar: Rethinking Credentials for Cybersecurity Careers
April 19
Webinar
https://www.nist.gov/news-events/events/2017/04/nice-webinar-rethinking-credentials-cybersecurity-careers

NCCoE Speaker Series: Cybersecurity 101 for Small Business
April 5
Rockville, MD
https://nccoe.nist.gov/events/nccoe-speaker-series-cybersecurity-101-small-business

Quest Baldrige Cybersecurity Pre-Conference Workshop
April 2
Baltimore, MD.
https://csrc.nist.gov/Events/2017/Quest-Baldrige-Cybersecurity-Pre-Conference-Worksh

MARCH 2017

Women in Cybersecurity (WiCyS) Conference
Editor Note: 2 members of the NICE team conducted a workshop on "Building the Cybersecurity Workforce: Careers, Coaching, and Collaboration" at this conference.
March 30-April 1
Tucson, Arizona
https://www.nist.gov/news-events/events/2017/03/women-cybersecurity-wicys-conference-tucson-arizona

ISPAB Meeting
March 29-31
Washington D.C.
https://csrc.nist.gov/Events/2017/ISPAB-March-2017-Meeting

Veterans in Cybersecurity Workforce Workshop (NICE cooperative agreement)
March 21
Rockville, MD

Spring 2017 Software and Supply Chain Assurance Forum
March 15-17
McLean, Virginia
https://csrc.nist.gov/Events/2017/Spring-2017-Software-and-Supply-Chain-Assurance-Fo

NICE Webinar: Building a Career Pathways System for Cybersecurity
March 15
Webinar
https://www.nist.gov/news-events/events/2017/03/nice-webinar-building-career-pathways-system-cybersecurity

30th Annual FISSEA Conference
March 14-15
CANCELLED due to inclement weather
https://www.nist.gov/news-events/events/2017/03/30th-annual-fissea-conference

Cybersecurity Framework Virtual Events
March 1
Webinar
https://www.nist.gov/news-events/events/2017/03/cybersecurity-framework-virtual-events

FEBRUARY 2017

NCCoE @ HIMSS 2017
February 19-23
Exhibit Booth and several speaking engagements
Orlando, Florida
https://nccoe.nist.gov/events/himss-annual-conference-exhibition

NICE Webinar: Best Practices for Educating, Training, Attracting, and Retaining Millennial
February 15
Webinar
https://www.nist.gov/news-events/events/2017/02/nice-webinar-best-practices-educating-training-attracting-and-retaining

Federal Computer Security Program Managers' Forum Meeting
February 14
NIST Gaithersburg, MD.
https://csrc.nist.gov/Events/2017/Federal-Computer-Security-Managers-Forum-Meeting

NIST Cybersecurity Program and NIST's NCCoE Program Exhibits at the 2017 RSA Conference
February 13-17
Exhibit Booths and demonstrations
San Francisco, California
https://www.nist.gov/news-events/events/2017/02/nist-exhibits-2017-rsa-conference

https://nccoe.nist.gov/events/rsa-conference-2017

JANUARY 2017

NICE Webinar: Cybersecurity Games: Building Tomorrow's Workforce
January 18
Webinar
https://www.nist.gov/news-events/events/2017/01/nice-webinar-cybersecurity-games-building-tomorrows-workforce

Cybersecurity, Research, Development and Implementation Industry Day/Pre-Solicitation Conference
January 13
NIST Gaithersburg, MD.
https://www.nist.gov/news-events/events/2017/01/cybersecurity-research-development-and-implementation-industry-daypre

DECEMBER 2016

Winter 2016 Software and Supply Chain Assurance Forum
December 13-15
McLean, Virginia
https://csrc.nist.gov/Events/2016/Winter-2016-Software-and-Supply-Chain-Assurance-Fo

NICE Webinar: Cybersecurity for Computer Science
December 7
Webinar
https://www.nist.gov/news-events/events/2016/12/nice-webinar-cybersecurity-computer-science

NCCoE Speaker Series: Understanding, Detecting & Mitigating Insider Threats
December 6
Rockville, MD
https://nccoe.nist.gov/events/nccoe-speaker-series-understanding-detecting-mitigating-insider-threats

3rd International Conference on Research in Security Standardisation (SSR)
December 5-6
NIST Gaithersburg, MD.
https://www.nist.gov/news-events/events/2016/12/3rd-international-conference-research-security-standardisation

NOVEMBER 2016

NICE Webinar: Building Your Cybersecurity Team with Apprenticeships
November 16
Webinar
https://www.nist.gov/news-events/events/2016/11/nice-webinar-building-your-cybersecurity-team-apprenticeships

NCCoE Speaker Series: Cybersecurity in the Health Community
November 9
Rockville, MD
https://nccoe.nist.gov/events/nccoe-speaker-series-suzanne-schwartz-fda-director-emergency-preparednessoperations-and

Forensics @ NIST 2016
November 8-9
NIST Gaithersburg, MD.
https://www.nist.gov/news-events/events/2016/11/forensics-nist-2016

7th Annual NICE Conference & Expo
November 1-2
Kansas City, Missouri
https://www.nist.gov/news-events/events/2016/11/7th-annual-nice-conference-expo-kansas-city-missouri

OCTOBER 2016

ISPAB Meeting
October 26-28
NIST Gaithersburg, MD.
https://csrc.nist.gov/Events/2016/ISPAB-October-2016-Meeting

Federal Computer Security Program Managers' Forum Meeting
October 26
NIST Gaithersburg, MD.
https://csrc.nist.gov/Events/2016/Federal-Computer-Security-Managers-Forum-Octobe

NSCI Seminar: CyberScience and CyberInfrastructure: A New Approach to Discovery in Science and Engineering
October 25
NIST Gaithersburg, MD.
https://www.nist.gov/news-events/events/2016/10/nsci-seminar-cyberscience-and-cyberinfrastructure-new-approach-discovery

Safeguarding Health Information: Building Assurance through HIPAA Security – 2016
October 19-20
Washington D.C.
https://www.nist.gov/news-events/events/2016/10/safeguarding-health-information-building-assurance-through-hipaa-security

Lightweight Cryptography Workshop 2016
October 17-18
NIST Gaithersburg, MD.
https://www.nist.gov/news-events/events/2016/10/lightweight-cryptography-workshop-2016

NCCoE Workshop: Derived PIV Credentials
October 11
NCCoE Facility (NIST) Rockville, MD.
https://nccoe.nist.gov/events/nccoe-workshop-derived-piv-credentials

https://csrc.nist.gov/Events/2016/NCCoE-Workshop-Derived-PIV-Credentials

National K-12 Cybersecurity Education Conference 2016
October 6-7
Arlington, Virginia
https://www.nist.gov/news-events/events/2016/10/national-k-12-cybersecurity-education-conference-2016-arlington-virginia

Maryland CyberDay 2016
October 5
Rockville, MD
https://www.mdcyber.com/reflections-maryland-cyber-day-2016/

Fall 2016 Software and Supply Chain Assurance Forum
October 4-5
McLean, Virginia
https://csrc.nist.gov/Events/2016/Fall-2016-Software-and-Supply-Chain-Assurance-Foru

APPENDIX C: OPPORTUNITIES TO ENGAGE WITH THE ITL CYBERSECURITY PROGRAM DURING FY 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

SSD Contact:
Dr. Ram Sriram
(301) 975-3507
ram.sriram@nist.gov

IAD Contact:
Dr. Shahram Orandi
(301) 975-3261
shahram.orandi@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:
https://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 https://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
grants@nist.gov

Funding opportunity information: https://www.nist.gov/about-nist/funding-opportunities