Information Technology Laboratory Newsletter

March—April 2017

Issue 146

INSIDE THIS ISSUE

RECORD-SETTING YEAR FOR ITL'S CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM

Comments Requested on Draft Update of Cybersecurity Framework and Cybersecurity Practice Guide

Revised Digital Identity Guidelines

Digital Library of Mathematical Functions a Valuable Resource

ITL Enables Healthcare Interoperability

Selected New Publications

Upcoming Technical Conferences

RECORD-SETTING YEAR FOR ITL'S CRYPTOGRAPHIC ALGORITHM VALIDATION PROGRAM

ITL's Cryptographic Algorithm Validation Program (CAVP) issued a record-setting 4,000 cryptographic algorithm validations in fiscal year 2016, bringing the total number of algorithm validations issued by the CAVP to 24,000. The CAVP provides validation testing of Federal Information Processing Standards (FIPS)-approved and NIST-recommended cryptographic algorithms and their individual components. A number of other milestones made it an exceptionally successful year for CAVP, including

- 4000th Advanced Encryption Standard (AES) validation,
- 2000th Triple Data Encryption Standard (TDES) validation,
- 1000th Digital Signature Algorithm (DSA) validation,
- 2000th RSA algorithm validation,
- 900th Elliptic Curve Digital Signature Algorithm (ECDSA) validation,
- 3000th Secure Hash Algorithm (SHA-1 and SHA-2) validation,
- 1000th Deterministic Random Bit Generator (DRBG) validation,
- 100th Key-based Key Derivation Function (KBKDF) validation.

This was also the first year the CAVP performed validation testing for the SHA-3 standard, allowing for 12 validations to be issued.

The CAVP validates cryptographic algorithms to provide assurance that they have been implemented correctly—complying with the specifications of the associated NIST cryptographic standards and uncovering implementation flaws caused by general coding errors. CAVP algorithm testing and validation is a prerequisite to the Cryptographic Module Validation Program (CMVP), which tests and validates cryptographic modules for conformance to FIPS 140-2, *Security Requirements for Cryptographic Modules.*

Vendors may use any of the NIST National Voluntary Laboratory Accreditation Program (NVLAP)-accredited Cryptographic and Security Testing (CST) Laboratories to test algorithm implementations. An algorithm implementation successfully tested by a laboratory and validated by NIST is added to an appropriate validation list, which identifies the vendor, implementation, operational environment, validation date, and algorithm details. Information regarding applying for laboratory accreditation, applicable fees, NVLAP Handbooks, and associated laboratory bulletins can be found at the NVLAP website.

See the CAVP website for more information on the FIPS-approved and NIST-recommended cryptographic algorithms currently validated by the CAVP, and the validation lists containing the validated cryptographic algorithm implementations. The CAVP and the CMVP are collaborative programs between NIST and the Government of Canada's Communication Security Establishment (CSE).

Comments Requested on Draft Update of Cybersecurity Framework and Cybersecurity Practice Guide

ITL recently issued a draft update to the Framework for Improving Critical Infrastructure Cybersecurity—also known as the Cybersecurity Framework. The updated framework provides new details on managing cyber supply chain risks, clarifies key terms, and introduces measurement methods for cybersecurity. April 10, 2017, is the deadline for comments on the draft Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. Comments should be sent to cyberframework@nist.gov (link sends e-mail).
The National Cybersecurity Center of Excellence (NCCoE) requests comments by April 17, 2017, on NIST Cybersecurity Practice Guide, Special Publication 1800-7, Situational Awareness for Electric Utilities.

Revised Digital Identity Guidelines

ITL recently released draft Special Publication (SP) 800-63-3: Digital Identity Guidelines for public review and comment. The document describes the techniques used by federal agencies to authenticate individuals and deploy identity solutions. ITL updated and simplified the guidelines to better align with Executive Order 13681, market advancements, and identity standards work occurring across the globe. Comments are due by March 31, 2017, on Github. Read the blog for more details: http://trustedidentities.blogs.govdelivery.com/2017/01/30/from-public-preview-to-public-draft-sp-800-63-is-open-for-comment/.

Digital Library of Mathematical Functions a Valuable Resource

The NIST Digital Library of Mathematical Functions (DLMF) is a valuable resource for scientists and engineers worldwide. The online DLMF and its associated printed NIST Handbook of Mathematical Functions (Cambridge University Press, 2010, 968 pages) has become the leading reference on the mathematical properties of the special functions of applied mathematics, which are the foundation for theoretical research in all of science and engineering.

The DLMF is the modern-day successor to the classic NBS Handbook of Mathematical Functions (M. Abramowitz and I. Stegun, eds., 1964), which is the most widely distributed and most highly cited publication in NIST's 117-year history. With already more than 2,900 citations in the technical literature (according to Google Scholar), the DLMF is on track to inherit the legacy of the fabled Abramowitz and Stegun Handbook.

ITL Enables Healthcare Interoperability

ITL recently participated in the 2017 Connectathon held in Cleveland, one of three events held annually in North America, Europe, and Asia. The major goal of the Connectathon is to promote the adoption of standards-based interoperability solutions defined by Integrating the Healthcare Enterprise (IHE) in commercially available healthcare IT systems. IHE is an initiative by healthcare professionals and industry that promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical needs in support of optimal patient care. *The Connectathon, the Health Information Technology industry's largest interoperability testing event, serves as an industry-wide testing event where developers of health information systems can test their implementations with those of other vendors.*
The North American Connectathon in Cleveland featured more than 97 systems from over 65 participating organizations. More than 3051 successful tests of 1052 different IHE Integration Profile/Actor pairs were performed and verified.

Ninety percent of the participants at the event used NIST tooling, provided and verified by NIST scientists from ITL's Software and Systems.

Division. ITL scientists also served as Connectathon monitors to verify test results on the show floor. Results of the Connectathon are published in the IHE Product Registry. This is a searchable database of IHE Integration Statements (conformance to IHE Profiles tested) as

Selected New Publications

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

By John Kelsey, Shu-Jen Chang, and Ray Perlner
NIST Special Publication 800-185
December 2016

This Recommendation specifies four types of SHA-3-derived functions: cSHAKE, KMAC, TupleHash, and ParallelHash, each defined for a 128- and 256-bit security strength. cSHAKE is a customizable variant of the SHAKE function, as 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 without trivial collisions. ParallelHash is a variable-length hash function that can hash very long messages in parallel.

Timing Challenges in the Smart Grid

By Jason Allnutt, Dhananjay Anand, Douglas Arnold, Allen Goldstein, Ya-Shian Li-Baboud, Aaron Martin, Cuong Nguyen, Robert Noseworthy, Ravi Subramaniam, and Marc Weiss
NIST Special Publication 1500-08
January 2017

Correct time and timing is one of the foundational elements in enabling the communication and orchestration of technologies for accurate and optimal wide-area monitoring, protection, and control in the power industry. NIST and IEEE-SA conducted a workshop to address the practical challenges that are currently being experienced in wide-area time synchronization. The workshop identified the challenges, the community of experts, and potential collaborators as well as key research priorities to guide future efforts for ensuring the integrity, availability, accuracy, and precision of timing requirements in power systems.

An Introduction to Privacy Engineering and Risk Management in Federal Information Systems

By Sean Brooks, Michael Garcia, Naomi Lefkovitz, Suzanne Lightman, and Ellen Nadeau
NISTIR 8062
January 2017

This document introduces the concepts of privacy engineering and risk management for federal information systems. These concepts establish the basis for a common vocabulary to facilitate better understanding and communication of privacy risk within federal information systems and the effective implementation of privacy principles. The publication introduces two key components to support the application of privacy engineering and risk management: privacy engineering objectives and a privacy risk model.

Mobile Application Vetting Services for Public Safety

By Gema Howell and Michael A. Ogata
NISTIR 8136
January 2017

The Middle Class Tax Relief Act of 2012 created the first nationwide, high-speed communications network dedicated for public safety, the Long Term Evolution (LTE) network. The network can equip first responders with a modern array of network devices. Mobile applications are an important resource that will be utilized by the network. However, current mobile application developers may not be equipped with the unique needs and requirements that must be met for operation on the network. This document provides an overview of existing mobile application vetting services and the features these services provide and how they relate to public safety's needs.

Code Complexity Makes Software Less Analyzable

By Charles D. De Oliveira, Elizabeth Fong, and Paul E. Black
NISTIR 8165
February 2017

ITL's Software Assurance Metrics and Tool Evaluation (SAMATE) team evaluated approximately 800 000 warnings from static analyzers. Results showed that elements called code complexities make the detection of warnings more difficult. Most tools cannot distinguish between the absence of a weakness and the presence of a weakness; that has been obscured in the code. This paper presents classes of code complexities. Understanding code complexity can assist in the development of coding guidelines for assuring that software is fully analyzable by static analyzers.

Examining the Copy and Paste Function in the Use of Electronic Health Records

By Svetlana Z. Lowry, Mala Ramaiah, Sandra Spickard Prettyman, Debora Simmons, David Brick, Ellen Deutsch, Lorraine Possanza, Ollie B. Gray, Betty A. Levine, Kinsey Gimbel, and Kyle Andrews
NISTIR 8166
January 2017

In collaboration with the ECRI Institute, ITL conducted a study of the copy and paste functions in electronic health records (EHRs). The study provided an in-depth examination of how healthcare practitioners utilize the copy and paste function in EHRs. The report provides recommendations for user interface design to ensure the safety-related usability for the copy and paste function.

Upcoming Technical Conferences

30th Annual Federal Information Systems Security Educators' Association (FISSEA) Conference

Dates: March 14-15, 2017
Place: NIST, Gaithersburg, Maryland
Sponsors: NIST and FISSEA
Cost: $105 with catering; $60 without catering

The theme of this year's conference is Securing the Future to Infinity and Beyond: 30 Years of Improving Cybersecurity through Awareness, Training, and Education. The audience will consist of managers responsible for information systems security training programs 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. FISSEA serves as a forum for the exchange of information about information security awareness, training, education, and certification.

NIST contact: Peggy Himes, peggy.himes@nist.gov

NSCI Seminar: Electrical and Physical Characterization of Nano- and Non-Linear Devices for Future Computing

Date: March 28, 2017
Place: NIST, Gaithersburg, Maryland
Sponsor: National Strategy Computing Initiative (NSCI) Committee
Cost: None

With the end of Moore's Law in sight, there is a great deal of angst in the information technology community over how computing can keep pace now that data is being generated and accumulated at an exponential rate. One solution is to perform exponentially more computation per unit of energy expended in a computer. This may very well require the exploitation of nonlinear dynamical systems to encode and process information in unconventional ways. Both nanoscale structures and neurons can display pathologically nonlinear responses such as chaos to a small stimulus, and in many ways the former can be used to emulate the latter. After a brief introduction to a couple of nonlinear electronic devices, the electronic and physical characterization tools and techniques that have been developed to characterize these systems will be described.

NIST contact: Barry Schneider, barry.schneider@nist.gov

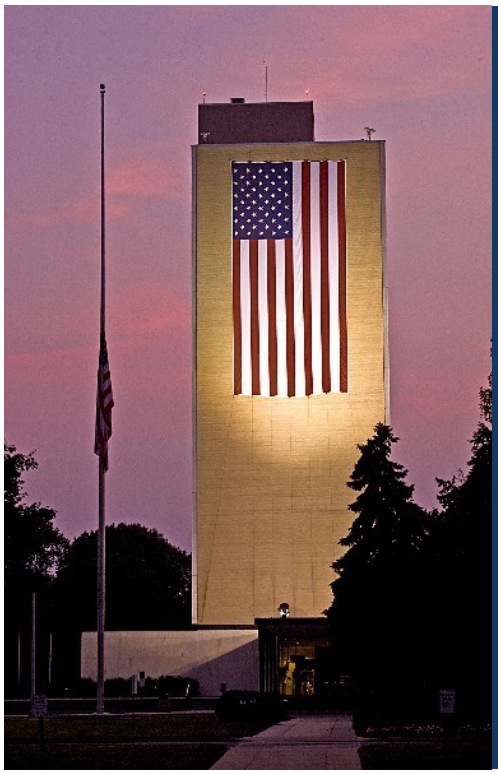
NSCI Seminar: Neuromorphic Silicon Learning Machines

Date: April 11, 2017
Place: NIST, Gaithersburg, Maryland
Sponsor: National Strategy Computing Initiative (NSCI) Committee
Cost: None

Learning and adaptation are key to natural and artificial intelligence in complex and variable environments. Advances in machine learning and system-on-chip very-large-scale-integration have led to the development of massively parallel silicon learning machines with pervasive real-time adaptive intelligence that begin to approach the efficacy and resilience of biological neural systems, and already exceed the nominal energy efficiency of synaptic transmission in the mammalian brain. This talk will highlight examples of neuromorphic learning systems-on-chips with applications in template-based pattern recognition, vision processing, and human-computer interfaces, and outline emerging scientific directions and engineering challenges in their large-scale deployment.

NIST contact: Barry Schneider, barry.schneider@nist.gov

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.



The NIST campus at Gaithersburg, MD.

Credit: NIST

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST). As a world-class measurement and testing laboratory encompassing a wide range of areas of computer science, mathematics, statistics, and systems engineering, our research program supports NIST's mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. ITL cybersecurity experts collaborate to develop cybersecurity standards, guidelines, and associated methods and techniques for federal agencies and industry. Our mathematicians and statisticians collaborate with measurement scientists across NIST to help ensure that NIST maintains and delivers the world's leading measurement capability. ITL computer scientists and other research staff provide technical expertise and development that underpins national priorities such as cloud computing, the Smart Grid, homeland security, information technology for improved healthcare, and electronic voting. We invite you to learn more about how ITL is enabling the future of the nation's measurement and standards infrastructure for information technology by visiting our website at http://www.itl.nist.gov.

ITL Editor: Elizabeth B. Lennon
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900
Phone: (301) 975-2832
Fax: (301) 975-2378
Email: elizabeth.lennon@nist.gov

TO SUBSCRIBE TO THE ELECTRONIC EDITION OF THE ITL NEWSLETTER, GO TO ITL HOMEPAGE