Information Technology Laboratory Newsletter


Credit: Shutterstock

September—October 2015

Issue 137

INSIDE THIS ISSUE

First NIST Cybersecurity Practice Guide Helps to Secure Patient Health Records

ITL's National Cybersecurity Center of Excellence (NCCoE) recently posted draft guidance for healthcare organizations seeking to better secure patient information when doctors, nurses, and other caregivers use mobile devices—smart phones and tablets—in conjunction with an electronic health record (EHR) system. NCCoE is seeking comments from the public. This document is the first in the new Special Publication series 1800, *NIST Cybersecurity Practice Guides,* which provides the information and instruction that IT security practitioners need to implement the NCCoE's example solutions using commercially available and open source technologies.

SP 1800-1, *Securing Electronic Health Records on Mobile Devices,* addresses the increasing use of mobile devices to store, process, and transmit patient information. When health information is stolen, inappropriately made public, or altered, healthcare organizations can face penalties and lose consumer trust, and patient care and safety may be compromised.

NCCoE built an environment that simulates interaction among mobile devices and an EHR system supported by the IT infrastructure of a medical organization. They considered a scenario in which a hypothetical primary care physician uses a mobile device to perform recurring activities such as sending a referral containing a patient's clinical information to another physician or sending an electronic prescription to a pharmacy. After determining the desired security characteristics and necessary components, the NCCoE issued a call in the *Federal Register* to submit letters of interest describing their products' capabilities. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build the example solution. Consortium members are Cisco, Intel, Maas360, MedTech Enginuity, Ramparts, RSA, and Symantec.

The practice guide:

- Maps security characteristics to standards and best practices from NIST and other standards organizations, and to the HIPAA Security Rule;
- Provides a detailed architecture and capabilities that address security controls;
- Facilitates ease of use through automated configuration of security controls;
- Addresses the need for different types of implementation, whether in-house or outsourced; and
- Provides a how-to for implementers and security engineers seeking to recreate the reference design.

Download the guide at the NCCoE website. Provide your feedback to HIT_NCCoE@nist.gov by **September 25, 2015**.

Secretary of Commerce Approves New and Updated Federal Information Processing Standards

The Secretary of Commerce recently approved two Federal Information Processing Standards (FIPS). FIPS 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, specifies the Secure Hash Algorithm-3 (SHA-3) family of functions on binary data. Each of the SHA-3 functions is based on an instance of the KECCAK algorithm that NIST selected as the winner of the SHA-3 Cryptographic Hash Algorithm Competition. FIPS 180-4, Secure Hash Standard, updates the current FIPS by specifying hash algorithms that can be used to generate digests of messages. The digests are used to detect whether messages have been changed since the digests were generated. The Applicability Clause of this standard was revised to correspond with the release of FIPS 202. The revision to the Applicability Clause approves the use of hash functions specified in either FIPS 180-4 or FIPS 202 when a secure hash function is required for the protection of sensitive unclassified information in federal applications.

ITL Advances the Adoption of Cloud Computing

NIST seeks to speed the adoption of cloud computing technology through collaborative work with industry, academia, and other government stakeholders involved in developing and disseminating vendor-neutral cloud computing standards and guidelines. To advance this goal, ITL recently hosted the eighth annual NIST Cloud Computing Forum and Workshop, an international event that focused on understanding the cloud computing needs and requirements of U.S. government agencies. Sponsored by the NIST Cloud Computing Program, the event gathered over 400 participants at NIST (and many more via web) who actively participated in discussions on cloud computing international standards, cloud security, forensics, research, service-level agreements, acquisition, interoperability, and portability. The program's long-term goal is to provide thought leadership and guidance around the cloud computing paradigm to catalyze a quick and secure adoption of cloud computing within industry and government. See more information on the NIST Cloud Computing Program.

ITL Co-Sponsors Major Conference on Computer Mathematics

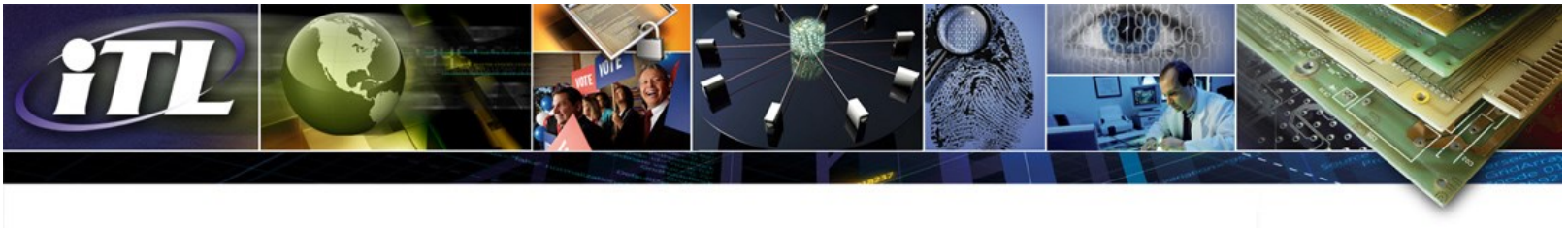
ITL recently co-sponsored the Conference on Intelligent Computer Mathematics (CICM) in Washington, D.C. The eighth conference in the series and the first to be held in the United States, CICM brings together researchers who seek to advance the use of computers and communication systems in mathematical research. During the week-long event, more than 65 participants from 15 countries shared recent advances on such topics as digital mathematical systems and libraries, mathematical knowledge management, and automated theorem proving. The proceedings of the conference appear as volume 9150 in the Springer series Lecture Notes in Artificial Intelligence.

Staff Accomplishments

NIST Fellow and Chief Statistician **Antonio Possolo** was elected to the Commission on Isotopic Abundances and Atomic Weights (CIAAW). Established in 1899, the CIAAW is the most prestigious and one of the oldest continuously serving scientific institutions. Former prestigious CIAAW members include Marie Curie, Nobel Prize winner in Chemistry in 1911, and Theodore Williams Richards, the first American to win the Nobel Prize winner in Chemistry in 1914.

Computer scientist **Kevin Mangold** received the Next Generation Award from the American National Standards Institute (ANSI) for his significant contributions to national and international standardization activities in biometrics and identity management, as well as ongoing commitment to the industry, the nation, and the enhancement of the global voluntary consensus standards system. The award is presented to outstanding members of ANSI who have been with the association for less than eight years.

This summer ITL and NIST's Communications Technology Laboratory hosted 35 students from 21 colleges and universities in the Summer Undergraduate Research Fellowship (SURF) program, which provides hands-on research experience in applied mathematics, statistics, software testing, computer security, information access, and networking.



Selected New Publications

JPEG 2000 CODEC Certification Guidance for 1000 ppi Fingerprint Friction Ridge Imagery
By Shahram Orandi, John Libert, Michael Garris, John Grantham, and Fred Byers
NIST Special Publication 500-300
June 2015

This document describes the procedure by which applications of JPEG 2000 CODECs will be evaluated with respect to conformance to the NIST guidance for compression of 1000 ppi (pixels per inch) friction ridge images as detailed in NIST Special Publication (SP) 500-289. It describes the attributes of a set of fingerprint images selected for conformance testing and the rationale for selection of these images based on both examiner assessment of image quality over increasing degrees of JPEG 2000 compression and relative fidelity based on computational metrics described SP 500-289 and supporting studies. The document also provides background behind the conformance testing, describes the CODEC pathways to be tested and the metrics used to measure compliance, and provides instructions on how to run the protocol and submit results to NIST for evaluation.

Conformance Testing Methodology Framework for ANSI/NIST-ITL 1-2011 Update: 2013, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information
By Christofer J. McGinnis, Dylan J. Yaga, and Fernando L. Podio
NIST Special Publication 500-304
June 2015

Conformance testing measures whether an implementation faithfully implements the technical requirements defined in a standard. Conformance testing provides developers, users, and purchasers with increased levels of confidence in product quality and increases the probability of successful interoperability. ITL developed a conformance testing methodology framework for ANSI/NIST-ITL 1-2011 Update: 2013, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information (AN-2013). This testing methodology framework defines the test assertions implemented within ITL's conformance test tool, which is designed to test implementations of AN-2013 transactions and promote biometrics conformity assessment efforts. This initial document includes comprehensive tables of AN-2013 requirements and test assertions for transaction-wide requirements, and Record Type 1 (which is required for all transactions). The tables of requirements and assertions indicate which assertions apply to the traditional encoding format, the National Information Exchange Model (NIEM)-compliant encoding format, or both encoding formats. The testing methodology framework defines and makes use of specific test assertion syntax which clearly defines the assertions associated with each requirement.

Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)
By Hildegard Ferraiolo, Ramaswamy Chandramouli, Nabil Ghadiali, Jason Mohler, and Scott Shorter
NIST Special Publication 800-79-2
July 2015

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

Random Number Generation Using Deterministic Random Bit Generators
By Elaine B. Barker and John M. Kelsey
NIST Special Publication 800-90A Rev 1
June 2015

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

Cardholder Authentication for the PIV Digital Signature Key
By W. Timothy Polk, Hildegard Ferraiolo, and David Cooper
NISTIR 7863
June 2015

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

gtklogger: A Tool for Systematically Testing Graphical User Interfaces
By Stephen Langer, Andrew Reid, Faical Congo, Rhonald Lua, and Valerie Coffman
NIST TN 1862
April 2015

This report describes a scheme for systematically testing the operation of a graphical user interface (GUI). The scheme provides a capability for generating event logs, which are recordings of a user session with the interface. These logs can be annotated with assertion statements, comparing reference test data with data retrieved by introspection on the GUI elements. Such an annotated log forms a test case, suitable for incorporation into a regression test suite.

Upcoming Technical Conferences

Safeguarding Health Information: Building Assurance through HIPAA Security – 2015
Dates: September 2-3, 2015
Place: Grand Hyatt, Washington, D.C.
Sponsors: NIST and Department of Health and Human Services Office of Civil Rights
Cost: $460 (with food); $228 (without food); $200 webcast

The conference will explore the current health information technology security landscape and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. The event will highlight the present state of health information security, and give practical strategies, tips, and techniques for implementing the HIPAA Security Rule.
NIST contact: Kevin Stine

2015 Cybersecurity Innovation Forum
Dates: September 9-11, 2015
Place: Walter E. Washington Convention Center, Washington, D.C.
Sponsors: NIST, NSA, and DHS
Cost: $270

This event brings government and industry together to focus on current, emerging, and future challenges, technologies, projects, solutions, and research in trusted computing, security automation, and information sharing. The technical program covers four tracks: Trusted Computing, Security Automation, Cyber Information Sharing and Research.
NIST contact: Melanie Cook

Best Practices in Cyber Supply Chain Risk Management
Dates: October 1-2, 2015
Place: NIST, Gaithersburg, Maryland
Sponsor: NIST
Cost: None

This workshop will provide insights on the state of practice of cyber supply chain risk management in several key industry sectors. It will focus on currently used tools, standards, and best practices, and how to establish a business case for integrating cyber supply chain risk management into organization's overall risk management processes.
NIST contact: Jon Boyens

BioImage Informatics Conference 2015
Dates: October 14-16, 2015
Place: NIST, Gaithersburg, Maryland
Sponsor: NIST
Cost: $304 (with catering); $165 (without catering service); $100 (full-time students)

This conference will bring together researchers and practitioners in the field of image informatics for the life sciences. The conference will cover a wide range of topics including applications to cell therapy, digital pathology, and regenerative medicine; data mining and machine learning of image information; advanced visualization of bioimages and image-derived information; storage and repositories of biological datasets; and other topics relevant to life science imaging and image informatics.
NIST contact: Peter Bajcsy

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

The NIST campus at Gaithersburg, MD.

Credit: NIST

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