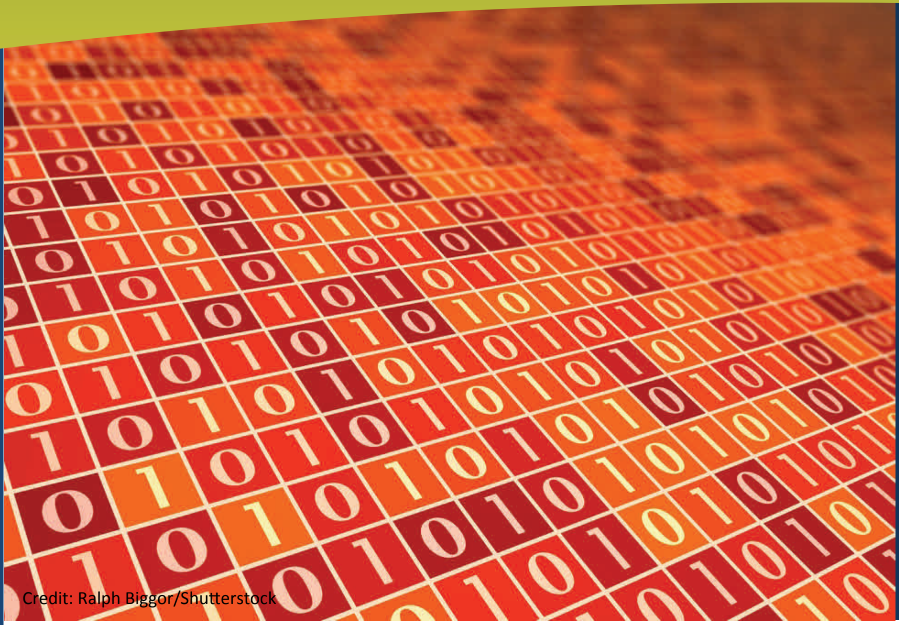
Information Technology Laboratory Newsletter

INSIDE THIS ISSUE



Credit: Ralph Biggor/Shutterstock

September—October 2013

Issue 125

ITL Launches the NIST Big Data Working Group

ITL recently launched a new NIST Big Data Working Group (NBD-WG), which has formed a community of interest from industry, academia, and government to define and articulate a common language and shared goals for Big Data. The group will develop consensus definitions, taxonomies, reference architectures, and a technology roadmap. The resulting vendor-neutral infrastructure framework will enable Big Data stakeholders to select the best analytics tools for their processing and visualization requirements, using the most suitable computing platform and cluster while allowing value-added from Big Data service providers.

Big Data is the term used to describe the deluge of data in our networked, digitized, sensor-laden, information-driven world. Commercial, academic, and government leaders concur on the remarkable potential of Big Data to spark innovation, fuel commerce, and drive progress. The availability of vast data resources carries the potential to answer questions previously out of reach. However, leaders also acknowledge the ability of Big Data to overwhelm traditional approaches, and introduce potential privacy concerns. The rate of growth of data volumes, speeds, and complexity is outpacing scientific and technological advances in data analytics, management, transport, and more.

Despite the widespread agreement on the opportunities and current limitations of Big Data, the lack of consensus on some fundamental questions confuses potential users and inhibits progress. How is Big Data different from the traditional data environments and related applications that we have encountered to date? What are the essential characteristics of Big Data environments? How do these environments integrate with currently deployed architectures? What are the central scientific, technological, and standardization challenges that need to be addressed to accelerate the deployment of robust Big Data solutions? The NIST Big Data Working Group will address these questions.

The NBD-WG has created five subgroups: Definitions and Taxonomies, Requirements, Security and Privacy, Reference Architecture, and Technology Roadmap. Participation in NBD-WG is open to everyone. For more information, see the NBD-WG website.

ITL Strengthens Digital Signature Standard for Federal Agency Use

The Secretary of Commerce recently approved a revision of Federal Information Processing Standard (FIPS) 186-4, Digital Signature Standard (DSS). The DSS approves the use of three digital signature algorithms: DSA, ECDSA, and RSA. This revision of the standard aligns the standard with other publications, such as NIST Special Publication 800-131A, Transitions: Recommendation for *Transitioning the Use of Cryptographic Algorithms and Key Lengths*, so that all NIST documents offer consistent guidance regarding the use of random number generators, which are used in DSS for the generation of digital signature keys.

Another update to the DSS concerns the use of prime number generators for the generation of RSA keys. Prime number generators require random seeds, which are used as initial values when searching for prime numbers. FIPS 186-3 specifically allowed saving these seeds only for use as evidence that the prime numbers were determined in an arbitrary manner; FIPS 186-4 permits saving these seeds for additional purposes, such as the regeneration of the prime numbers, if required.

ITL Promotes Healthcare IT Interoperability

ITL recently provided infrastructure and tests for the 2013 European Connectathon in Istanbul, Turkey, one of three Integrating the Healthcare Enterprise (IHE)-sponsored 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 IHE in commercially available healthcare IT systems.

The IHE European Connectathon is a five-day event whose main purpose is testing the interoperability and connectivity of healthcare IT systems. In a vast hall that is hardwired for high-speed Internet, more than 300 IT engineers come together in a casual but intensely concentrated setting to interconnect more than 100 systems and collaboratively solve problems. Participants state that identifying and fixing a system bug during an IHE Connectathon is one-tenth as expensive and difficult as debugging a system once it is installed at a hospital or clinic. Scientists from ITL's Software and Systems Division provided infrastructure and tests for the event. Seventy-four vendors ran 2,212 tests to verify 920 IHE profiles/actor pairs. ITL scientists also served as Connectathon monitors to verify test results on the Connectathon 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 published by vendors with IHE capabilities in their product offerings. ITL's contributions to this effort result in significant savings of cost and time to market for vendors of healthcare IT systems.

ITL Hosts Visit of Math Undergraduates

A group of nine undergraduate students representing five minority-serving colleges and universities recently visited NIST to learn how mathematics is used in science and engineering research. The students were participants in the Math SPIRAL (Summer Program In Research And Learning) program of the University of Maryland's College of Computer, Mathematical and Physical Sciences. SPIRAL is a multiyear program funded by the National Science Foundation and the National Security Agency to bring gifted college undergraduates from underrepresented groups to the College Park Campus. During the six-week summer session, students participate in intensive classroom work built around applications and opportunities in the mathematical sciences. They work with research teams on campus and see a wide range of career opportunities through tours and special lectures. The visit to NIST was sponsored by the ITL Diversity Committee in association with ITL's Applied and Computational Mathematics Division and Statistical Engineering Division.

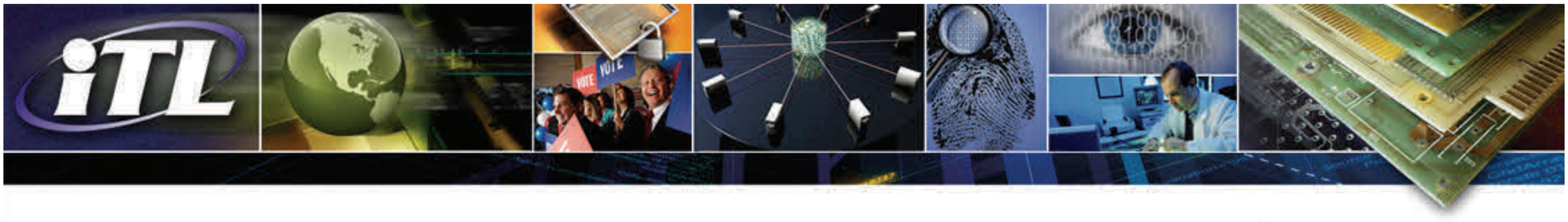
Staff Recognition

Ronald Boisvert, Chief of ITL's Applied and Computational Mathematics Division, recently completed an unprecedented three terms (nine years) as Co-Chair of the Publications Board of the Association for Computing Machinery (ACM). ACM is the world's largest educational and scientific society in the computing field. Its publications include more than 40 research journals, 8 magazines, and 26 newsletters, as well as more than 450 conference proceedings volumes each year.

Patrick Grother, of ITL's Information Access Division, received a American National Standards Institute 2013 Leadership and Service Award from the American National Standards Institute (ANSI). He received the Edward Lohse Information Technology Medal, which "recognizes outstanding efforts to foster cooperation among the bodies involved in global IT standardization."

ITL Deputy Standards Liaison **Elaine Newton** has been named one of three recipients of the ANSI Next Generation Award for demonstrating vision, leadership, dedication and significant contributions to standards activities since 2006. The ANSI Next Generation Award is presented to outstanding members who have been engaged with the association for less than eight years.

Murugiah Souppaya and **Michael Bartock**, part of a team from ITL's National Cybersecurity Center of Excellence (NCCoE), Intel, and RSA, received the 2013 Innovation Award from RSA for their proof of concept and implementation of "Trusted Geolocation in the Cloud." The implementation uses RSA Archer commercial enterprise and risk management solutions and dashboard/ reporting and integration functionality to demonstrate that a compute node in a virtualized environment can be measured at launch time, continuously monitored, and have its physical location and level of compliance determined. This helps businesses feel confident in the security of virtual machines in a hosted infrastructure and cloud technology.



Selected New Publications

NIST Cloud Computing Standards Roadmap
NIST Cloud Computing Standards Roadmap Working Group
NIST Special Publication 500-291 Revision 2
July 2013

The Federal Chief Information Officer (CIO) designated NIST to accelerate the federal government's secure adoption of cloud computing by leading efforts to develop standards and guidelines in close consultation and collaboration with standards bodies, the private sector, and other stakeholders. The NIST Cloud Computing Standards Roadmap Working Group surveyed the existing standards landscape for interoperability, performance, portability, security, and accessibility standards/models/studies/use cases/conformity assessment programs, etc., relevant to cloud computing. Using this available information, current standards, standards gaps, and standardization priorities are identified within this document.

Guide to Enterprise Patch Management Technologies
By Murugiah Souppaya and Karen Scarfone
NIST Special Publication 800-40 Revision 3
July 2013

This publication assists organizations in understanding the basics of enterprise patch management technologies. It provides an overview of enterprise patch management technologies and briefly discusses metrics for measuring the technologies' effectiveness and for comparing the relative importance of patches.

Biometric Specifications for Personal Identity Verification
By Patrick J. Grother, Wayne J. Salamon, and Ramaswamy Chandramouli
NIST Special Publication 800-76-2
July 2013

Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, called for new standards to be adopted governing interoperable use of identity credentials to allow physical and logical access to federal government locations and systems. NIST developed *Federal Information Processing Standard (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors*, which defines procedures and specifications for issuance and use of an interoperable identity credential. This document, a companion document to *FIPS 201*, describes technical acquisition and formatting specifications for the PIV system and establishes minimum accuracy specifications for deployed biometric authentication processes.

Guide to Malware Incident Prevention and Handling for Desktops and Laptops
By Murugiah Souppaya and Karen Scarfone
NIST Special Publication 800-83 Revision 1
July 2013

Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system. This publication provides recommendations for improving an organization's malware incident prevention measures.

Guideline for the Implementation of Coexistence for Low Frequency Narrowband Power Line Communication Standards in the Smart Grid
David H. Su, Editor
NISTIR 7943

The Smart Grid Interoperability Panel (SGIP) established the Priority Action Plan 15 (PAP 15) in 2009 to address the harmonization of new Power Line Communication (PLC) standards and their coexistence specifications. This report presents PAP15's recommendation on the implementation of coexistence mechanisms for Narrowband (NB)-PLC standards.

IREX VI Temporal Stability of Iris Recognition Accuracy
By Patrick J. Grother, James R. Matey, Elham Tabassi, George W. Quinn, and Michael Chumakov
NISTIR 7948
July 2013

Stability is a required definitional property for a biometric to be useful. Quantitative statements of stability are operationally important as they dictate reenrollment schedules, e.g., of a face on a passport. We quantify time variation in iris recognition accuracy in two ways. First we produce rate-of-change estimates for up to 122,000 frequent travelers using a fixed iris recognition system for up to 9 years. Second, we apply iris recognition algorithms to the images of 217 individuals used in a Notre Dame study. The algorithms produce pupil dilation and exposed iris area measures which we relate to recognition outcomes.

IREX VI: Part 1, Evaluation of Iris Identification Algorithms
By George W. Quinn, Patrick Grother, and Meilee L. Ngan
NISTIR 7949
July 2013

IREX IV aims to provide a fair and balanced scientific evaluation of the performance of automated iris recognition algorithms. IREX IV evaluated the performance of 66 identification (i.e., one-to-many) algorithms submitted by 12 companies and universities. IREX IV investigated the use of cost models for application-specific algorithm optimization. The goal is to see if algorithm developers can improve performance when given advanced knowledge of the costs of identification errors.

Toward a Shared Approach for Ensuring Patient Safety with Enhanced Workflow Design for Electronic Health Records (EHRs) – Summary of the Workshop
By Svetlana Lowry, Mala Ramaiah, A. Ozok, A.P. Gurses, M.C. Gibbons, D. Brick, E.S. Patterson, and V.R. Lewis
NISTIR 7952
July 2013

In April 2013, NIST sponsored the EHR Usability and Patient Safety Roundtable: Supporting Patient Safety through EHR Design. At the workshop, representatives of government, EHR developers, EHR users, and academics identified common ground on challenges and aspirations to improve patient safety, usability, and human factors regarding workflows in the use of electronic health records. Achieving these objectives is necessary to enhance safe and effective care to all patients and increase the rate of adoption of electronic health records in the United States.

Upcoming Technical Conferences

4th Cybersecurity Framework Workshop
Dates and Place: September 11-13, 2013, University of Texas at Dallas, Richardson, Texas
Sponsor: NIST; Cost: None

NIST will present a draft Preliminary Cybersecurity Framework for discussion. Draft materials will be posted on the conference website for review by late August 2013; participants are asked to review posted materials prior to arrival at the workshop and to come prepared to offer substantive input on the level of guidance, presentation of the Cybersecurity Framework, implementation, and governance.
NIST contact: Suzanne Lightman

4th Annual NICE Workshop: Navigating the National Cybersecurity Education InterState Highway
Dates and Place: September 17-19, 2013, NIST, Gaithersburg, Maryland
Sponsors: National Initiative for Cybersecurity Education (NICE), NIST; Cost: $85

The workshop will showcase cybersecurity programs and public outreach activities for the State level in industry, education, and government sectors. The event will feature keynote speakers, panel discussions, poster sessions, and an interactive State(s) view on cybersecurity education, best practices, and competitions.
NIST contact: Magdalena Benitez

2013 Biometric Consortium Conference & Biometric Technology Expo
Dates and Place: September 17-19, 2013, Tampa Convention Center, Tampa, Florida
Sponsors: NIST, National Security Agency, and AFCEA International; Cost: $595 - $695

The conference will focus on biometric technologies for defense, homeland security, identity management, border crossing, and electronic commerce. The conference will feature four tracks, panel discussions, workshops, and a biometrics tutorial. The keynoter will be Jeremy Grant, Senior Executive Advisor for Identity Management, National Strategy for Trusted Identities in Cyberspace (NSTIC), ITL.
NIST contact: Fernando Podio

The Intersection of Cloud and Mobility
Dates and Place: October 1-3, 2013, NIST, Gaithersburg, Maryland
Sponsor: NIST; Cost: None

As part of its continuing cloud computing series, NIST/ITL is hosting a new forum on Cloud and Mobility. Join experts in the fields of cloud, mobility, and measurement for thought-provoking plenary talks, panel presentations, facilitated breakout discussion, poster sessions, and networking on federal perspectives on cloud and mobility; current state of cloud and mobility intersections; path forward to a federated mobile cloud; and challenges for cloud and mobility. On October 3rd, the Cloud Computing Forensic Science Workshop will cover the future of cloud forensics, challenges for cloud forensics, and the path forward for cloud forensics.
NIST contacts: Michaela Iorga and Frederic de Vaulx

Fundamentals of Uncertainty Analysis
Dates and Place: October 28-31, 2013, NIST, Gaithersburg, Maryland
Sponsor: NIST; Cost: $1,275

This short course covers many aspects of the propagation of uncertainty using the methods outlined in the JCGM Guide to the Expression of Uncertainty in Measurement. Exercise and hands-on applications will use functions for uncertainty analysis from the free software package, metRology, written for the open source R statistical computing environment. The functions will be accessed via an Excel graphical user interface, as a free add-in.
NIST contact: Will Guthrie

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 in Gaithersburg, Maryland.

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