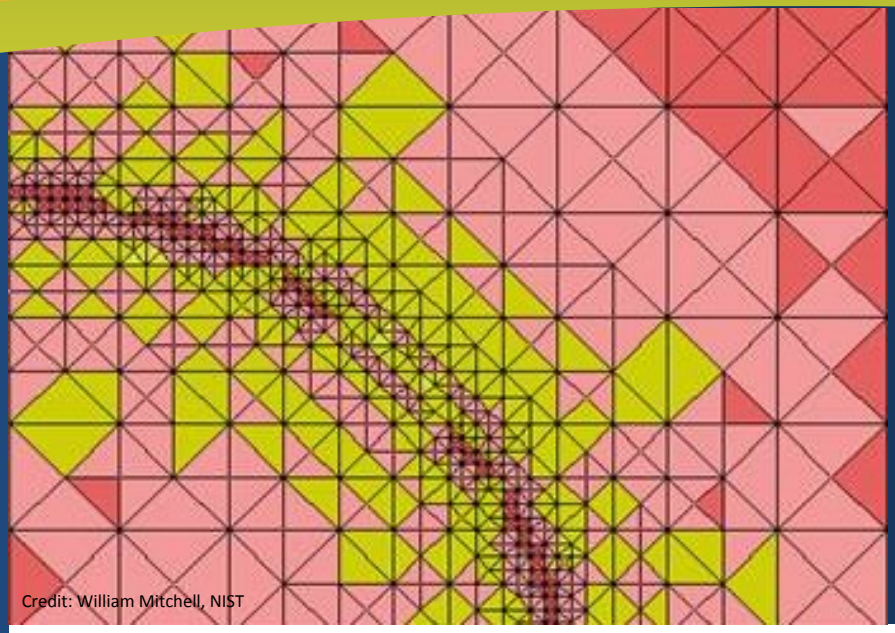
Information Technology Laboratory Newsletter



Credit: William Mitchell, NIST

November—December 2014

Issue 132

INSIDE THIS ISSUE

ITL SCIENCE DAY HIGHLIGHTS TECHNICAL ACHIEVEMENTS AND FUTURE DIRECTIONS OF THE LABORATORY

On October 1, 2014, the third annual ITL Science Day brought together mathematicians, statisticians, computer scientists, and other technical staff from around the laboratory to celebrate their recent technical achievements, initiate collaborations with other divisions in the laboratory, and look ahead to new challenges. ITL Director Charles Romine gave the opening address, in which he categorized the technical work of the laboratory as outlined in the ITL Strategic Plan. The three overarching components of ITL's technical work are:

- Fundamental research in mathematics, statistics, and information technology;
- Applied IT research and development; and
- Standards development and technology transfer.

Romine then gave examples of recent technical achievements in quantum information, statistical metrology, computational science, metrology for modeling and simulation, networking, cyber-physical systems, data, human language technology, cybersecurity, biometrics, standards and interoperability, and forensics. He suggested expanded future NIST collaborations in advance manufacturing/materials genome; quantum information science and engineering; forensic science; cyber-physical systems; and communications technology. He concluded his address by outlining areas of expected future ITL growth:

- Network function virtualization and software-defined networks;
- Standards and measurements to accelerate data-driven innovation;
- Privacy;
- Metrology for scientific computing; and
- Metrology for assurance of IT products and services.

The day included talks by speakers from the National Institutes of Health, the National Science Foundation, and the Department of Transportation; eight talks by ITL staff participating in the NIST Building the Future program; and two lively poster sessions with a total of 62 posters by ITL technical staff describing their work. The program concluded with announcement of the winning posters:

- Charles Hagwood and Javier Bernal: Testing Equality of Cell Populations Based on Shape and Geodesic Distance;
- Yvonne Kemper and Isabel Beichl: Approximating the Chromatic Polynomial;
- Dhananjay Anand and William Harrison: Data Fusion for Command Decision Support; and
- Yee-Yin Choong, Desire Banse, Haiying Guan, Charles Sheppard, and Mary Theofanos: Ten-Print Fingerprint Self-Captures: Graphics-Only User Guidance without Language.

ITL Focuses on Privacy Engineering

ITL recently held a 2nd Workshop on Privacy Engineering. The purpose of the workshop was to gather feedback on an ITL-developed draft set of privacy engineering objectives and risk model to address the lack of well-developed models, technical standards, and best practices in privacy risk management. The workshop attendance included over 80 privacy experts and advocates, software developers, and designers, as well as legal and policy experts and academics. Participants agreed with the need for a common vocabulary and taxonomy to allow privacy professionals and engineers to better facilitate the integration of privacy with design and engineering decisions. Using the feedback from the workshop and other comments received, ITL is developing a publication on privacy engineering. The document will present the fundamental concepts of a privacy engineering framework appropriate for use by a wide variety of public and private sector organizations. A draft document will be released for public comment in fiscal year 2015.

ITL Researchers Contribute to Secure Smartphone Apps for the Military

ITL computer scientists joined with engineers from other NIST operating units to develop and deliver secure smartphone apps for use by the military in Afghanistan. The project was funded by the Transformative Apps program of the Defense Advanced Research Projects Agency (DARPA), which defined the objective: "Develop a diverse array of militarily-relevant software applications using an innovative new development and acquisition process." The four-year project involved determining the requirements of soldiers in the field, creating a unique security architecture for smartphones, and testing the performance of the apps. ITL contributions included expertise in cybersecurity and software performance evaluation. The NIST researchers received the 2014 Government Computer News Award for Information Technology Excellence for their work. For complete details of the project, see the NIST article.

ITL Develops Secure Hash Algorithm 3 (SHA-3) Draft Standard

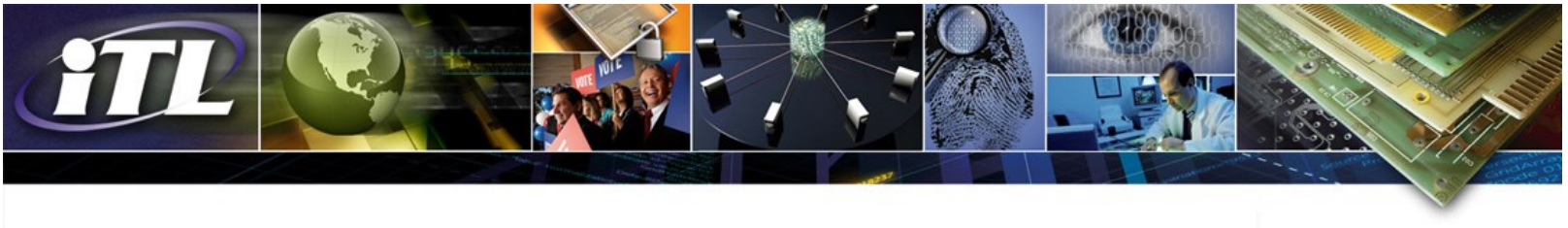
Last spring ITL announced Draft Federal Information Processing Standard (FIPS) 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, based on the winning algorithm in the SHA-3 Competition: KECCAK. To advance the development of the standard, ITL hosted a SHA-3 Workshop at the University of California, Santa Barbara, to obtain public feedback on the proposed Standard, as well as possible applications and modes of operation based on SHA-3 that are being considered for standardizing.

The workshop opened with an overview and status update on the proposed Standard, followed by sessions on security analysis and implementations of KECCAK, hash modes, a panel discussion on parallelizable hashing, and an invited talk by the KECCAK designer on the "KECCAK Code Package." ITL presented its plan on the development of several SHA-3-based special publications: authenticated encryption; KECCAK-based Message Authentication Code (KMAC); guidance on the use of Extendible Output Functions (XOFs); and domain extensions. Follow the development of the standard at this website.

ITL Contributes Statistical Expertise to Standards for Optical Medical Imaging

ITL statisticians and other members of the NIST Innovations in Measurement Science (IMS) Optical Medical Imaging (OMI) project recently organized the NIST Workshop on Standards for the Advancement of Optical Medical Imaging. The keynote speech addressed the need for standards in translational optical medical imaging. More talks along this theme focused on topics such as phantom development and validation, image performance metrics, and uncertainty analysis for optical imaging in translational research. The program included talks on newer developments such as photoacoustic and molecular imaging. Also discussed were some of the most popular optical platforms in optical coherence tomography (OCT), the technology currently preferred by ophthalmologists worldwide, but which still lacks required image performance metrics and standards.

The workshop highlighted key areas of NIST expertise and competencies developed over the last five years of the IMS OMI project. These included improvements and breakthroughs in a number of spectroscopic technologies for hyperspectral biomedical imaging and the development and implementation of algorithms for analyzing and processing these images.



Selected New Publications

The Twenty-Second Text REtrieval Conference Proceedings (TREC 2013)
Ellen Voorhees, Editor
NIST Special Publication 500-302
September 2014

This report constitutes the proceedings of the Twenty-Second Text REtrieval Conference (TREC 2013) held in Gaithersburg, Maryland, on November 19--22, 2013. The conference was cosponsored by NIST and the Defense Advanced Research Projects Agency (DARPA).

Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography
By Elaine Barker, Lily Chen, and Dustin Moody
NIST Special Publication 800-56B, Revision 1
September 2014

This Recommendation specifies key-establishment schemes using integer factorization cryptography, based on ANS X9.44, Key-establishment using Integer Factorization Cryptography [ANS X9.44], which was developed by the Accredited Standards Committee (ASC) X9, Inc.

BIOS Protection Guidelines for Servers
By Andrew Regenscheid
NIST Special Publication 800-147B
August 2014

Modern computers rely on fundamental system firmware, commonly known as the Basic Input/Output System (BIOS), to facilitate the hardware initialization process and transition control to the hypervisor or operating system. The guidelines in this document include requirements on servers to mitigate the execution of malicious or corrupt BIOS code. They apply to BIOS firmware stored in the BIOS flash, including the BIOS code, the cryptographic keys that are part of the Root of Trust for Update, and static BIOS data. This guide provides server platform vendors with recommendations and guidelines for a secure BIOS update process.

Computer Security Division 2013 Annual Report
Patrick O'Reilly, Editor; Chris Johnson, Doug Rike, and Greg Witte, Co-Editors; and Lorie Richards
NIST Special Publication 800-170
June 2014

Title III of the E-Government Act of 2002, entitled the Federal Information Security Management Act (FISMA) of 2002, requires ITL 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. ITL's Computer Security Division provides standards and technology that protect information systems against threats to the confidentiality, integrity, and availability of information and services. During Fiscal Year 2013, division staff developed and applied high-quality, cost-effective security and privacy mechanisms that improved information security across the federal government and the greater information security community.

Guidelines for Smart Grid Cybersecurity
By Victoria Pillitteri and Tanya Brewer
NISTIR 7628 Rev. 1
September 2014

This three-volume report presents an analytical framework that organizations can use to develop effective cybersecurity strategies tailored to their particular combinations of smart grid-related characteristics, risks, and vulnerabilities. Organizations in the diverse community of smart grid stakeholders can use the methods and supporting information in this report as guidance for assessing risk and identifying and applying appropriate security requirements. This approach recognizes that the electric grid is changing from a relatively closed system to a complex, highly interconnected environment. Each organization's cybersecurity requirements should evolve as technology advances and as threats to grid security inevitably multiply and diversify.

Challenges and Benefits of a Methodology for Scoring Web Content Accessibility Guidelines (WCAG) 2.0 Conformance
By Frederick Boland and Elizabeth Fong
NISTIR 8010
September 2014

The World Wide Web (W3C) Web Accessibility Initiative (WAI) has developed comprehensive guidance on promoting web accessibility. As part of the WAI, the Web Content Accessibility Guidelines (WCAG) 2.0 specifies success criteria for evaluating the conformance of web content to the guidelines. This paper presents a methodology to score adherence of a web page to WCAG 2.0 conformance requirements. The paper summarizes challenges and benefits, and provides a detailed description of research on a sample web page.

IREX V: Instructional Material for Iris Image Collection
By George W. Quinn, James Matey, Elham Tabassi, and Patrick Grother
NISTIR 8013
July 2014

This document provides guidance for the proper collection of iris images. Problems that occur during image acquisition can lead to poor quality samples. If the subject was looking down or blinking at the moment of capture, the image should be rejected and a new one acquired. Such problems are fairly simple and straightforward to correct, but require attentiveness on the part of the camera operator. If an image of a closed eye is accepted without scrutiny, no amount of post-capture processing can recover the lost information. For this reason, certain procedures should be followed to ensure that only good quality samples are collected.

Measurement Uncertainties of Three Score Distributions and Two Thresholds with Data Dependency
By Jin Chu Wu, Alvin F. Martin, Craig S. Greenberg, and Raghu N. Kacker
NISTIR 8025
September 2014

NIST conducts an ongoing series of Speaker Recognition Evaluations (SRE). Recently a new paradigm was adopted to evaluate the performance of speaker recognition systems in which three distributions of target, known non-target, and unknown non-target scores, as well as two thresholds were employed. The new detection cost function was defined to be an average of the two weighted sums of the probabilities of type I and type II errors corresponding to the two decision thresholds. In addition, data dependency due to multiple uses of the same subjects is involved. The measurement uncertainties, i.e., the standard errors of the detection cost function, improved as a result of taking account of the data dependency.

Upcoming Technical Conferences

Cybersecurity for Direct Digital Manufacturing Symposium
Date: February 3, 2015
Place: NIST, Gaithersburg, Maryland
Sponsor: NIST
Cost: TBD

This symposium will explore cybersecurity needed for direct digital manufacturing. Speakers from industry, academia, and government will discuss the state of the industry, cybersecurity risks and solutions, and implications for Information and Communications Technology (ICT) supply chain risk management.
NIST contact: Celia Paulsen

Hands-on Workshop on Assessing and Reporting Measurement Uncertainty
Dates: March 18-20, 2015
Place: Anaheim, California
Sponsor: NIST
Cost: TBD

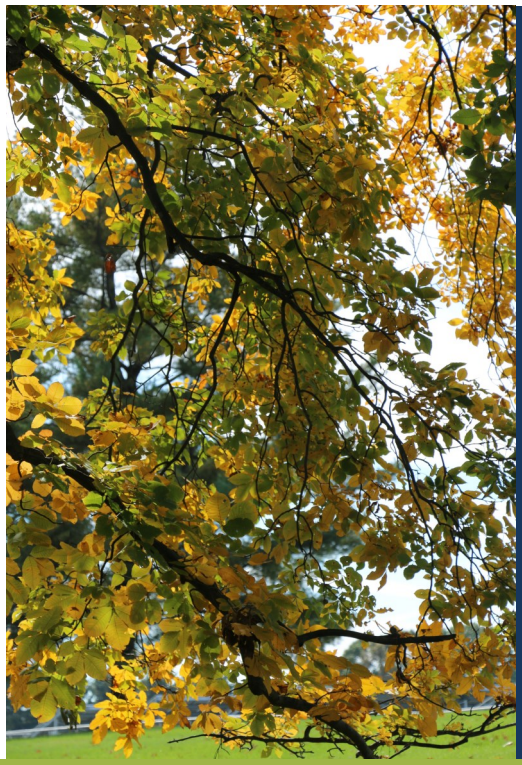
This short course covers many aspects of the propagation of uncertainty using the methods outlined in the *JCGM Guide to the Expression of Uncertainty in Measurement*. Exercises and hands-on applications will use functions for uncertainty analysis from the free software package, metRology, written for the open-source R statistical computing environment. The functions can be accessed directly using R or via metRology for Microsoft Excel, a graphical user interface available as a free add-in. This short course is being given as part of the 2015 Measurement Science Conference.
NIST contact: Will Guthrie

FISSEA Annual Conference
Dates: March 24-25, 2015
Place: NIST, Gaithersburg, Maryland
Sponsors: NIST and FISSEA
Cost: TBD

At the annual Federal Information Systems Security Educators' Association (FISSEA) conference, attendees will gain a better understanding of current cybersecurity projects, emerging trends, and initiatives; awareness and training ideas, resources, and contacts; new techniques for developing and conducting training; networking opportunities; professional development; and an opportunity to meet industry partners at the vendor exhibit.
NIST contact: Peggy Himes

Workshop on Cybersecurity in a Post-Quantum World
Dates: April 2-3, 2015
Place: NIST, Gaithersburg, Maryland
Sponsor: NIST
Cost: TBD

The advent of practical quantum computing will break all commonly used public key cryptographic algorithms. In response, NIST is researching cryptographic algorithms for public key-based key agreement and digital signatures that are not susceptible to cryptanalysis by quantum algorithms. NIST is holding this workshop to engage academic, industry, and government stakeholders. The workshop will be co-located with the 2015 International Conference on Practice and Theory of Public-Key Cryptography, which will be held March 30 - April 1, 2015. NIST seeks to discuss issues related to post-quantum cryptography and its potential future standardization.
NIST contact: Dustin Moody



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

Credit: Katherine Green, NIST