

Information Technology Laboratory Newsletter

INSIDE THIS ISSUE

Cybersecurity Framework for Critical Infrastructure Advances

ITL Develops the First Data-Logger/Playback System for Integrated Clinical Environment

NIST Researchers Publish Case Study of Usability Metrics

Staff Recognition

NIST Cloud Computing Team Collaborates to Create a Standardized Cloud Computing Service-Level Agreement

NIST/SEMATECH E-Handbook of Statistical Methods: A Valuable Resource for Scientists and Engineers

Selected New Publications

Upcoming Technical Conferences



Credit: Andrea Danti/Shutterstock

November—December 2013

Issue 126

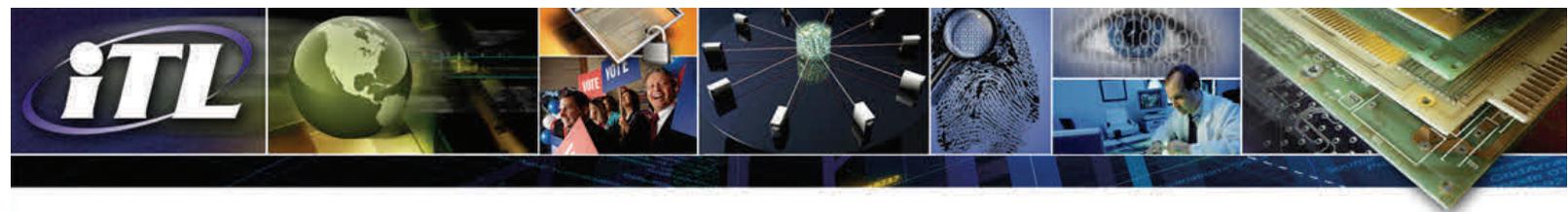
Cybersecurity Framework for Critical Infrastructure Advances

ITL continues to advance the development of a cybersecurity framework to strengthen the resilience of our nation's critical infrastructure. We recently released a [Preliminary Cybersecurity Framework](#) for public review and comment. ITL is developing the framework based on information gathered from stakeholders over the past six months including a Request for Information in the Federal Register dated February 26, 2013, and a series of five public workshops held at various locations throughout the United States.

The most recent workshop was held on November 14-15, 2013, at North Carolina State University (NCSU) in Raleigh, North Carolina. The workshop engaged stakeholders on the preliminary framework; participants discussed strategies around implementation and future governance of the framework. Following the welcome plenary with Dr. Charles Romine, ITL Director, and Dr. Randy Woodson, Chancellor, NCSU, ITL staff gave an overview of the framework. A second panel addressed privacy and civil liberties issues, followed by topic-specific working sessions in the afternoon. Day two of the workshop included a panel giving perspectives from the telecom sector, a panel on adoption considerations for the framework, and a closing session on next steps.

NIST is developing the framework under Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, which calls for a voluntary cybersecurity framework that provides for a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" for assisting organizations responsible for critical infrastructure services to manage cybersecurity risk. Consisting of standards, guidelines, and methodologies that promote the protection of information systems supporting critical infrastructure operations, the framework will facilitate the wide adoption of best practices to increase cybersecurity across all sectors and industry types. The flexible and cost-effective approach of the framework will assist owners and operators of critical infrastructure in managing cybersecurity risk while ensuring business confidentiality and individual privacy.

As announced in the [Federal Register](#) notice of October 29, 2013, we are seeking your input and comments on the Preliminary Cybersecurity Framework. Electronic comments should be submitted in Microsoft Word or Excel formats to: csfcomments@nist.gov, with the Subject line: Preliminary Cybersecurity Framework Comments. Written comments concerning the preliminary Framework may be sent to: Information Technology Laboratory, ATTN: Adam Sedgewick, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930. All comments will be posted at http://csrc.nist.gov/cyberframework/preliminary_framework_comments.html without change or redaction, so commenters should not include information they do not wish to be posted (e.g., personal or business information). **Comments are due by December 13, 2013.** Complete information is available in the Federal Register notice.



ITL Develops the First Data-Logger/Playback System for Integrated Clinical Environment

In collaboration with the Center for Integration of Medicine and Innovative Technology/Massachusetts General Hospital, ITL developed and demonstrated the first Data-Logger/Playback prototype system based on the ASTM 2761 Integrated Clinical Environment (ICE) Standard. The demonstration took place at a Medical Device Plug-and-Play Program event at the National Institutes of Health (NIH). The Data-Logger/Playback module allows for capturing/reviewing the appropriate data in an integrated clinical environment and enables various forensic, research, and educational use cases.

Led by electronics engineer Kamran Sayrafian, a team of ITL researchers developed the prototype as part of the Medical Device Interoperability project within ITL's Health Information Technology Program. The module was implemented based on an ITL-developed scalable middleware technology, i.e., NDFS-II (NIST Data Flow System 2). The Data-Logger/Playback system was presented along with other technical research demonstrations from NIH's Quantum Medical Device Interoperability project collaborators during the two-day event, which displayed the latest achievements in medical device interoperability in a plug-and-play environment. See more information about the [NIH event](#). More detail about NIST's [Health Information Technology](#) Program is also available.

NIST Researchers Publish Case Study of Usability Metrics

Usability researchers Mary Theofanos, Office of Data and Informatics, Material Measurement Laboratory, and Yee-Yin Choong and Brian Stanton, of ITL's Information Access Division, recently published a case study entitled *Measuring the Effect of Feedback on Fingerprint Capture*. The work is included as Chapter 10 in a new book, *Measuring the User Experience, Collecting, Analyzing, and Presenting Usability Metrics* by Tom Tullis and Bill Albert. The preeminent metrics book in the usability field, the new release is the second edition of a well-received and respected reference, *Measuring the User Experience*. This was the first book that focused on how to quantify the user



Credit: NIST

experience. The second edition includes new material on how recent technologies have made it easier and more effective to collect a broader range of data about the user experience. It presents new metrics and examines how new technologies can refine user experience measurement. The book also contains new research, updated examples, and six new case studies including the ITL case study.

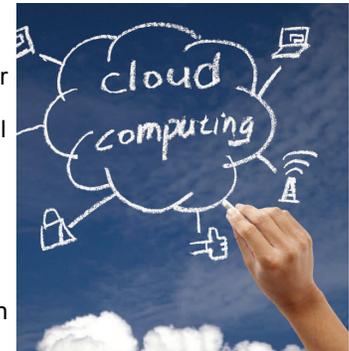
Staff Recognition

Nien Fan Zhang, Statistical Engineering Division, was one of a team of four NIST researchers who were recognized by R&D Magazine with a 2013 R&D 100 Award. The NIST team received the award for their invention of quantitative hybrid metrology (QHM), a new statistical method to determine the sizes of

nanoscale transistor features on semiconductor chips. The award was presented at a ceremony in Orlando, Florida, on November 7, 2013.

NIST Cloud Computing Team Collaborates to Create a Standardized Cloud Computing Service-Level Agreement

The NIST Cloud Computing Team worked with the International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) Joint Technical Committee 1 Subcommittee 38, Distributed Application Platforms and Services (DAPS), to create a new standardization project within Working Group 3 on Cloud Computing Service-Level Agreements (SLAs). The new ISO/IEC JTC1 Standard being developed is 19086 - Cloud computing – Service-Level Agreement (SLA) Framework and Terminology.

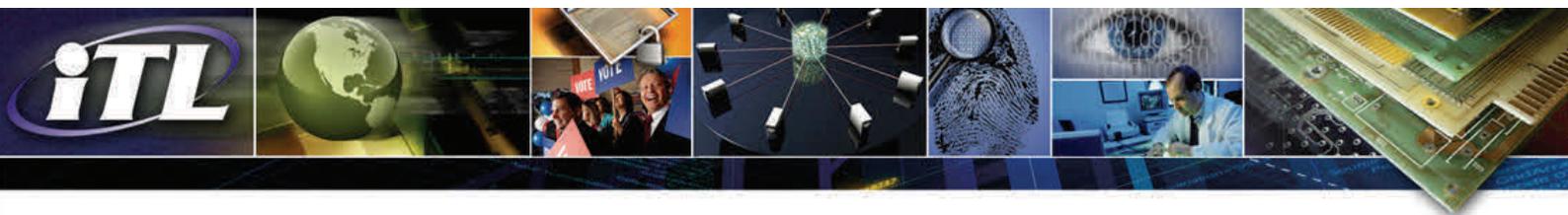


Credit: Tom Wang/Shutterstock

While SLAs for telecommunication services and IT outsourcing are mature and commonly used, adapting them for cloud computing is nontrivial. SLAs for cloud computing must be able to handle large numbers of users sharing geographically diverse computing resources that can change rapidly and dynamically. There are currently no standards for Cloud Computing SLAs and little commonality between SLAs from differing cloud providers. This new project will create an international standard on the building blocks used to create SLAs and will provide an overview of SLAs for cloud services, identification of the relationship between the master service agreement and the SLA, SLA components that can be used within a framework to build SLAs, and terms and metrics commonly used in SLAs for cloud services. The standard will benefit both cloud service providers and cloud customers.

NIST/SEMATECH E-Handbook of Statistical Methods: A Valuable Resource for Scientists and Engineers

ITL offers a valuable resource for scientists and engineers who want to use statistical procedures in their work in an efficient and effective manner. The [NIST/SEMATECH e-Handbook of Statistical Methods](#) is a web-based reference for those users without statistical experience to design their own experiments and conduct appropriate analyses. The handbook also serves as an educational tool to facilitate the understanding of statistical procedures by scientists, engineers, and other users who need to interpret statistical information. For more information on the development of the handbook, see the [handbook website](#).



Selected New Publications

[Electronic Authentication Guideline](#)

By William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, and Emad A. Nabbus
NIST Special Publication 800-63-2, Aug. 2013

This recommendation provides technical guidelines for federal agencies implementing electronic authentication and is not intended to constrain the development or use of standards outside of this purpose. The recommendation covers remote authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks. It defines technical requirements for each of four levels of assurance in the areas of identity proofing, registration, tokens, management processes, authentication protocols and related assertions. The document supersedes NIST SP 800-63-1.

[Secure Domain Name System \(DNS\) Deployment Guide](#)

By Ramaswamy Chandramouli and Scott Rose
NIST Special Publication 800-81-2
September 2013

The Domain Name System (DNS) is a distributed computing system that enables access to Internet resources by user-friendly domain names rather than IP addresses, by translating domain names to IP addresses and back. The DNS infrastructure is made up of computing and communication entities called Name Servers, each of which contains information about a small portion of the domain name space. The domain name data provided by DNS is intended to be available to any computer located anywhere in the Internet. This document provides deployment guidelines for securing DNS within an enterprise.

[A Framework for Designing Cryptographic Key Management Systems](#)

By Elaine Barker, Miles Smid, Dennis Branstad, and Santosh Chokhani
NIST Special Publication 800-130
August 2013

This Framework for Designing Cryptographic Key Management Systems (CKMS) contains topics that should be considered by a CKMS designer when developing a CKMS design specification. For each topic, there are one or more documentation requirements that need to be addressed by the design specification. Thus, any CKMS that addresses each of these requirements would have a design specification that is compliant with this Framework.

[Effects of Decomposition Levels and Quality Layers with JPEG 2000 Compression of 1000 ppi Fingerprint Images](#)

By John M. Libert, Shahram Orandi, and John D. Grantham
NISTIR 7939
August 2013

As part of NIST's research efforts to support development of the FBI Next Generation Identification (NGI) systems, this study evaluates effects on image fidelity of wavelet transform decomposition and quality layer options for JPEG 2000 compression of 1000 ppi fingerprint images. First, a suite of 1000 ppi fingerprints are subjected to encoding specifying from three to eight levels of DWT decomposition. Decoded images are compared to non-compressed source images and fidelity loss is

evaluated by certified latent fingerprint examiners as well as by several automated computational fidelity metrics. Fidelity losses among the six decomposition level options result in no statistically significant differences among assessments of image degradation by trained fingerprint examiners. Computational metrics find statistically significant fidelity differences, with lowest error for five and six DWT decompositions. A second experiment is also described in the report.

[A Vision of Cyber-Physical Cloud Computing for Smart Networked Systems](#)

By Eric Simmon, Kyoung-Sook Kim, Eswaran Subrahmanian, Ryong Lee, Frederic de Vault, Yohei Murakami, Koji Zettsu, and Ram D. Sriram
NISTIR 7951
July 2013

A key aspect of the next generation Smart Networked System (SNS) is the bridge between the physical and virtual world. These systems that tightly interlink the cyber and physical worlds are often referred to as Cyber-Physical Systems (CPS). A CPS is the "integration of computation with physical processes" and uses sensors and actuators to link the computational systems to the physical world. The modern CPS inspires a new vision of "computing as a physical act" where the real world is monitored through sensors that transfer sensing data into the cyberspace where cyber applications and services use the data to affect the physical environment in real time. The interlinked networks of sensors, actuators, and processing devices create a vast network of connected computing resources, things, and humans that we will refer to as a Smart Networked System. There are five technologies that are core to the concept of a SNS: networked computer systems, real-time systems, wireless sensor/actuator networks, social networks, and cloud computing services.

[Measurement Uncertainty in Cell Image Segmentation Data Analysis](#)

By Jin Chu Wu, Michael Halter, Raghu N. Kacker, John T. Elliot, and Anne L. Plant
NISTIR 7954
August 2013

Cell image segmentation is a part of quantitative studies regarding cell movement and cell behavior, and it plays a critical role in molecular biology and cellular biochemistry. Therefore, it is fundamentally important to evaluate the performance levels of cell image segmentation algorithms. In our previous study, the performance metrics for cell image segmentation algorithms were proposed. The sampling variability can result in measurement uncertainties. In this article, the uncertainty of the measure, i.e., the total error rate, in the cell image segmentation is computed in terms of standard error and 95 % confidence interval using bootstrap method as well as an analytical method. Examples are provided.



Upcoming Technical Conferences

[Software Asset Management Building Block Workshop](#)

Date: December 5, 2013
Place: 9600 Gudelsky Drive, Rockville, Maryland
Sponsor: National Cybersecurity Center of Excellence (NCCoE)
Cost: None; registration required

This workshop will review the Continuous Monitoring Software Asset Management (SAM) Building Block. The building block proposes techniques for meeting SAM challenges. As envisioned in this building block, SAM requires a standardized approach that provides an integrated view of software throughout its life cycle. Security researchers, security practitioners, and system integrators will find this workshop valuable.

NIST contact: [Tim McBride](#)

[2014 Cybersecurity Innovation Forum and Expo](#)

Dates: January 28-30, 2014
Place: Baltimore Convention Center, Baltimore, Maryland
Sponsors: National Cybersecurity Center of Excellence (NCCoE), with primary participating organizations: Department of Homeland Security, NIST, and the National Security Agency
Cost: \$495

The forum will cover the existing threat landscape and provide presentations and keynotes on current and emerging practices, technologies and standards. The 2014 forum will provide action-oriented outputs to fuel voluntary principle-driven consensus-based standards efforts, create opportunities for industry growth and drive research activities, and define use cases for subsequent exploration, which in turn will feed back into the coming years' forums, continually evolving the state of the art.

NIST contact: [Melanie Cook](#)

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.

[Cryptographic Key Management Issues & Challenges in Cloud Services](#)

By Ramaswamy Chandramouli, Michaela Iorga, and Santosh Chokani
NISTIR 7956
September 2013

To interact with various services in the cloud and to store the data generated/processed by those services, several security capabilities are required. Based on a core set of features in the three common cloud services - Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), we identify a set of security capabilities needed to exercise those features and the cryptographic operations they entail. An analysis of the common state of practice of the cryptographic operations that provide those security capabilities reveals that the management of cryptographic keys takes on an additional complexity in cloud environments compared to enterprise IT environments.

[Conformance Test Architecture and Test Suite for ANSI/NIST-ITL 1-2011 NIEM XML](#)

Encoded Transactions
By Fernando L. Podio, Dylan J. Yaga, and C.J. McGinnis
NISTIR 7957
August 2013

The latest version of the ANSI/NIST-ITL standard was published in November 2011 (AN-2011). In addition to specifying Record Types in traditional encoding, the standard includes the specification of National Information Exchange Model (NIEM) Extensible Markup Language (XML) encoding and an associated schema. ITL developed a Conformance Test Architecture (CTA) and Test Suite (CTS) called BioCTS for AN-2011 NIEM XML designed to test implementations of AN-2011 NIEM XML encoded transactions. This document discusses the test software design including the XML Data Structures used and Classes implemented. It addresses the testing phases and the format of the test results, as well as the user interface and key usability features implemented in this version of the test tool.



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 in Gaithersburg, Maryland.

Credit: NIST

TO SUBSCRIBE TO THE ELECTRONIC EDITION OF THE ITL NEWSLETTER, GO TO [ITL HOMEPAGE](#)