

# Information Technology Laboratory Newsletter

## INSIDE THIS ISSUE

ITL Focuses on Pervasive Information Technology

Digital Library of Mathematical Functions Team Cited for IT Innovation

Selected Publications

Upcoming Technical Conferences



© Nicholas McIntosh

November 2011

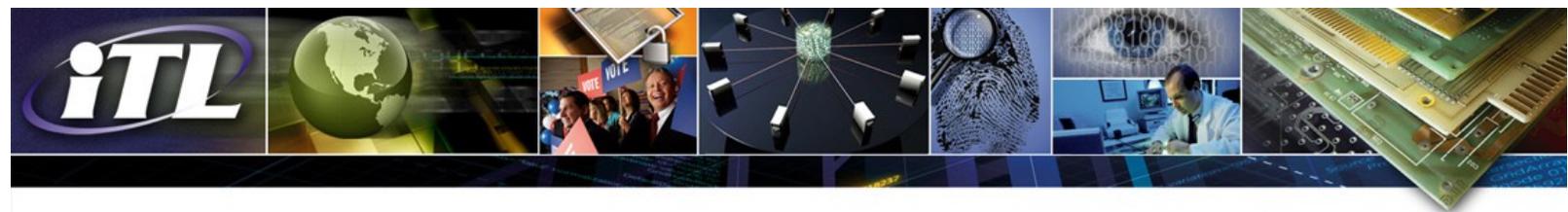
Issue 116

## ITL Focuses on Pervasive Information Technology

Recent advances in microelectronics and wireless networking are moving closer to turning devices once thought of as science fiction into clinical reality. Ultra-small medical sensors/actuators can be either worn or implanted inside the body to collect or deliver a variety of medical information and services. The networking ability between these body devices and also possible integration with existing information technology (IT) infrastructure could result in a pervasive environment that can convey health-related information between the user at any location or time and his or her healthcare provider. This flexibility for greater physical mobility and continuous health awareness directly translates into a significantly higher healthcare experience and therefore, higher quality of life. Current ITL projects include Body Area Network technology and medical device interoperability.

Body Area Network (BAN) is a technology that allows communication between ultra-small and ultra-low-power intelligent sensors/devices that are located on the body surface or implanted inside the body. In addition, the wearable/implantable nodes can also communicate to a controller device that is located in the vicinity of the body. These radio-enabled sensors can be used to continuously gather a variety of important health and/or physiological data (i.e., information critical to providing care) wirelessly. Radio-enabled implantable medical devices offer a revolutionary set of possible applications, including smart pills for precision drug delivery, intelligent endoscope capsules, glucose monitors, and eye pressure sensing systems. Similarly, wearable sensors allow for various medical/physiological monitoring (e.g., electrocardiogram, temperature, respiration, heart rate, and blood pressure), disability assistance, etc. A simple example of a BAN application would be a device equipped with a built-in reservoir and pump. This device could administer just the right amount of insulin to a diabetic person based on wirelessly received glucose level measurements from another body sensor. Having such novel uses in pervasive healthcare, BAN is regarded as a promising interdisciplinary technology that could have a huge impact on advancing health IT and telemedicine with its widespread commercialization.

ITL researchers are also working on efforts that promote standards-based medical device interoperability and communication. From acute care clinical settings, to vital-sign monitoring, and devices that make telemedicine more accurate and effective, medical devices are playing an ever-increasing role in transforming healthcare delivery. These devices have the ability to capture critical medical data, available (perhaps) multiple times per second, essential to a patient's care. However, for the most part, they are unable to communicate with one another and offer almost no plug-and-play interoperability to allow them to work in combinations tailored to a patient's needs. Lack of reference implementations for existing device interface standards and unanswered questions regarding the safety and performance of networked systems-of-systems are among the challenges to achieve such interoperability. A standard interoperable framework will allow novel clinical solutions to be safely and efficiently incorporated. The Web site is [here](#).



## Digital Library of Mathematical Functions Team Cited for IT Innovation

The NIST Digital Library of Mathematical Functions (DLMF) was selected for recognition as an Outstanding Information Technology Achievement in Government for 2011 by Government Computer News (GCN). Available [here](#), the DLMF is the online interactive successor to the classic NBS Handbook of Mathematical Functions (M. Abramowitz and I. Stegun, eds.) published in 1964. The DLMF provides reference data on the special functions of applied mathematics in a concise, usable form needed in a wide variety of fields, from the physical sciences to engineering, biology and finance. The online reference features interactive graphics, math-aware search capabilities, and a rich set of internal and external links.

According to GCN, these awards “have come to symbolize the best and most notable IT accomplishments in advancing the work of government agencies.” Ten projects were selected for recognition this year from more than 200 nominations. The selection was based on “the degree of innovation in the technology plan carried out, the quality of the leadership that carried the project to fruition, and the degree to which a given IT project improved an agency’s ability to operate more efficiently or serve the public more effectively.” Other awardees this year include an app from the City of Boston that enables citizens to request city services from their smart phones and the IT infrastructure that supports the Transportation Security Administration’s secure flight program.

NIST staff members cited for this achievement are Daniel Lozier, Frank Oliver, Ronald Boisvert, Bruce Miller, Bonita Saunders, Marjorie McClain, Abdou Youssef, Qiming Wang, and Brian Antonishek of the Information Technology Laboratory and Charles Clark of the NIST Physical Measurement Laboratory. The project team was formally honored at the 24th Annual GCN Awards Gala, October 19, 2011, at the Ritz-Carlton, Tysons Corner in McLean, Virginia.



## Selected New Publications

### [The Nineteenth Text REtrieval Conference \(TREC 2010\) Proceedings](#) E. M. Voorhees and Lori P. Buckland, Editors

NIST Special Publication 500-297  
October 2011

This document presents the proceedings of the Nineteenth Text REtrieval Conference (TREC 2010) held in November 2010 at NIST.

### [NIST Cloud Computing Reference Architecture](#)

By Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf

NIST Special Publication 500-292  
September 2011

The adoption of cloud computing in the US Government (USG) and its implementation depend upon a variety of technical and nontechnical factors. A fundamental reference point, based on the NIST definition of Cloud Computing, is needed to describe an overall framework that can be used governmentwide; this document presents the NIST Cloud Computing Reference Architecture (RA) and Taxonomy (Tax) that will accurately communicate the components and offerings of cloud computing.

### [Information Security Continuous Monitoring for Federal Information Systems and Organizations](#)

By Kelley Dempsey, Arnold Johnson, Alicia Clay Jones, Angela Orebaugh, Matthew Scholl, and Kevin Stine

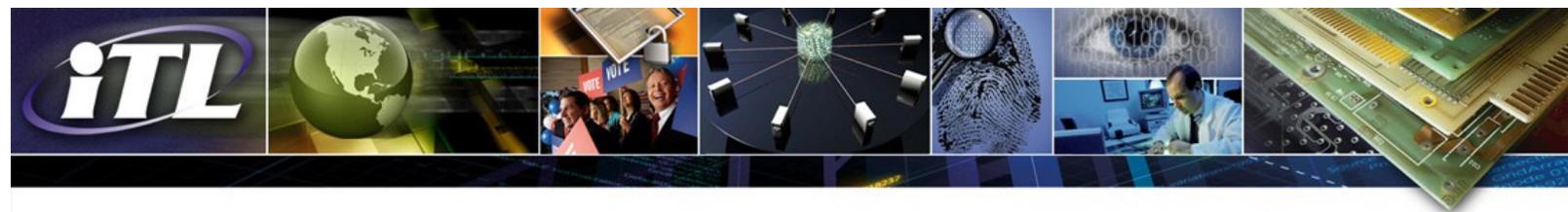
NIST Special Publication 800-137  
September 2011

This guideline assists organizations in the development of a continuous monitoring strategy and the implementation of a continuous monitoring program providing visibility into organizational assets, awareness of threats and vulnerabilities, and visibility into the effectiveness of deployed security controls. It provides ongoing assurance that planned and implemented security controls are aligned with organizational risk tolerance as well as the information needed to respond to risk in a timely manner should observations indicate that the security controls are inadequate.

### [Common Platform Enumeration: Naming Specification Version 2.3](#)

By Brant A. Cheikes, David Waltermire, and Karen Scarfone  
NISTIR 7695  
August 2011

This report defines the Common Platform Enumeration (CPE) Naming version 2.3 specification. The CPE Naming specification is a part of a stack of CPE specifications that support a variety of use cases relating to IT product description and naming. The CPE Naming specification defines the logical structure of names for IT product classes and the procedures for binding and unbinding these names to and from machine-readable encodings. The report also defines and explains the requirements that IT products must meet for conformance with the CPE Naming version 2.3 specification.



## Selected New Publications

### [Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters](#)

By Andrew Regenscheid and G. Beier  
NISTIR 7711  
September 2011

This document outlines the basic process for the distribution of election material including registration material and blank ballots to Uniformed and Overseas Citizen Absentee Voting Act (UOCAVA) voters. It describes the technologies that can be used to support the electronic dissemination of election material along with security techniques – both technical and procedural – that can protect this transfer. The purpose of the document is to inform Election Officials about the current technologies and techniques that can be used to improve the delivery of election material for UOCAVA voters.

### [Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs](#)

By Anoop Singhal and Ximming Ou  
NISTIR 7788  
August 2011

To more accurately assess the security of enterprise systems, one must understand how vulnerabilities can be combined and exploited to stage an attack. Composition of vulnerabilities can be modeled using probabilistic attack graphs, which show all paths of attacks that allow incremental network penetration. Attack likelihoods are propagated through the attack graph, yielding a novel way to measure the security risk of enterprise systems. This methodology based on probabilistic attack graphs can be used to evaluate and strengthen the overall security of enterprise networks.

### [Trust Model for Security Automation Data 1.0 \(TMSAD\)](#)

By Harold Booth and Adam Halbardier  
NISTIR 7802  
September 2011

This report defines the Trust Model for Security Automation Data 1.0 (TMSAD), which permits users to establish integrity, authentication, and traceability for security automation data. Since security automation data is primarily stored and exchanged using Extensible Markup Language (XML) documents, the focus of the trust model is on the processing of XML documents. The trust model is composed of recommendations on how to use existing specifications to represent signatures, hashes, key information, and identity information in the context of an XML document within the security automation domain.

### [NIST Special Database 32 – Multiple Encounter Dataset II \(MEDS-II\)](#)

By Craig I. Watson and N. Orlans  
NISTIR 7807  
August 2011

This document and associated dataset is an update to the Multiple Encounter Dataset I (MEDS-I), originally published by ITL in May 2010. The MEDS is a test corpus organized from an extract of submission files of deceased persons with prior multiple encounters. A submission file is an electronic file containing biographic and biometric data recorded during an encounter with an individual. The submission files conform to the

specifications defined by the Electronic Biometric Transmission Specification (EBTS) extension to the American National Standards Institute (ANSI)/NIST Information Technology Laboratory (ITL)-1-2007 standard.

### [Defining AFIS Latent Print “Lights-Out”](#)

By Vladimir Dvornychenko and S. Meagher  
NISTIR 7811  
September 2011

The term “lights-out” has been used within the AFIS 10-print fingerprint operations to suggest that no human intervention is involved. Before this term can be applied in the forensic latent print operation, a more in-depth understanding is required. The end-to-end latent print examination process is presented and seven tiers are described for potential “lights-out” scenarios. A major objective of this paper is to define these seven tiers and establish a common understanding for each. Doing so will enable future testing of latent print “lights-out” scenarios to be clearly defined and operational implementations and consequences associated with each tier to be fully understood.

### [Iris Quality Calibration and Evaluation \(IQCE\): Evaluation Report](#)

By Elham Tabassi, Patrick Grother, and Wayne Salamon  
NISTIR 7820  
September 2011

Iris is rapidly gaining acceptance and support as a viable biometric. United States Visitor and Immigrant Status Indicator Technology (US-VISIT), Personal Identity Verification (PIV) and Unique Identification Authority of India (UID) programs are either using or considering iris as their secondary or primary biometric for verification. While there are several academic publications addressing the problem of iris image quality, NIST Iris Quality Calibration and Evaluation (IQCE) is the first public challenge in iris image quality aimed at identifying iris image quality components that are algorithm- or camera-agnostic. This evaluation supports homeland security, counter-terrorism, and border control applications by enhancing reliability and accuracy of iris recognition, and significantly improves requirement planning and system design.

### [A Comparison of hp-adaptive Strategies for Elliptic Partial Differential Equations \(long version\)](#)

By William Mitchell and Marjorie McClain  
NISTIR 7824  
October 2011

The hp version of the finite element method (hp-FEM) combined with adaptive mesh refinement is a particularly efficient method for solving partial differential equations because it can achieve a convergence rate that is exponential in the number of degrees of freedom. Hp-FEM allows for refinement in both the element size,  $h$ , and the polynomial degree,  $p$ . Like adaptive refinement for the  $h$  version of the finite element method, a posteriori error estimates can be used to determine where the mesh needs to be refined, but a single error estimate cannot simultaneously determine whether it is better to do the refinement by  $h$  or by  $p$ . Several strategies for making this determination have been proposed over the years. In this paper, we summarize these strategies and present the results of a numerical experiment to study the convergence properties of these strategies.

# Upcoming Technical Conferences

## Federal Information Systems Security Educators' Association (FISSEA) Conference

Dates: March 27-29, 2012

Place: NIST, Gaithersburg, Maryland

Sponsors: FISSEA and NIST

The conference theme is *A New Era in Cybersecurity Awareness Training and Education*. Tracks and presentations will focus on current projects, emerging trends, and initiatives in cybersecurity awareness, training, and education.

NIST contact: Peggy Himes, 301/975-2489, [peggy.himes@nist.gov](mailto:peggy.himes@nist.gov)

FISSEA Web site [here](#).

## Privacy-Enhancing Cryptography Workshop

Dates: December 8-9, 2011

Place: NIST, Gaithersburg, Maryland

Cost: \$165

The purpose of this workshop is to explore the many privacy-enhancing applications that should follow from the ability to operate on encrypted data without decrypting it. Cryptographers need guidance regarding what processes and procedures can benefit from privacy-enhancing technologies. Technology consumers need a better understanding of the new functionalities of privacy-enhancing technologies and their potential. Everyone needs a better feel for which technologies are, or can be made to be, cost-efficient.

NIST contact: Rene Peralta, 301/975-8702, [rene.peralta@nist.gov](mailto:rene.peralta@nist.gov)

Conference Web site [here](#).

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.



*If you are interested in receiving our newsletter, send your name, organization, and business mailing address to:*

*ITL Newsletter  
National Institute of Standards and Technology  
100 Bureau Drive, Stop 8900  
Gaithersburg, MD 20899-8900*

*You will be placed on this mailing list only.*

*The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of new information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our Web site is <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  
E-mail: [elizabeth.lennon@nist.gov](mailto:elizabeth.lennon@nist.gov)

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

NIST/Denease Anderson