

ITL NEWSLETTER FOR MAY 2009

ITL DEVELOPS TEST SUITES FOR ELECTRONIC VOTING SYSTEMS

ITL recently released for public review and comment, draft test suites for the next generation of electronic voting systems. The test suites are designed to assure voters, election officials, and manufacturers of electronic voting systems of the security, usability, and reliability of future voting systems. Test laboratories will be able to use these public test suites to help evaluate the conformance of voting systems to requirements in the Voluntary Voting System Guidelines (VVSG), which were developed by ITL scientists for the U.S. Election Assistance Commission under a mandate from the 2002 Help America Vote Act. The current version of the guidelines is VVSG 2005; the test suites will be for use with the next generation of voting systems, known as VVSG Next Iteration (VVSG-NI).

Public test suites will provide numerous benefits for all parties involved in the development, testing, and use of electronic voting systems. Manufacturers of electronic voting equipment, such as optical scanners and touch screens, can utilize the test suites to develop products that conform to the precise specifications. Testing laboratories can use the test suites to produce results that are consistent, transparent, and less costly. Finally, election officials and voters will have increased confidence in electronic voting systems that conform to VVSG-NI requirements.

The test suites are available at <http://vote.nist.gov/voting-system-test-suites.htm>, along with guidelines for reviewers. Comments must be received by NIST by **July 1, 2009**.

For more information on ITL's work to improve the nation's voting systems, see <http://vote.nist.gov>.

ITL Implements Immersive Visualization Environment for RF Propagation from Medical Implants

The Implant Communication System project has successfully implemented an immersive visualization environment that can be used as a scientific instrument which enables the observation of radio frequency (RF) propagation from medical implants inside a human body. This virtual environment allows for more natural interaction between experts with different backgrounds, such as engineering and medical sciences.

Body area networks which consist of RF-enabled wearable and implantable sensory nodes are poised to be a promising interdisciplinary technology with novel uses in pervasive health information technology. However, numerous challenges including size, cost, energy source, sensing/actuator technology, and transceiver design still need to be resolved. Knowledge of the propagation media is a key step toward a successful transceiver design. Such information is typically gathered by conducting physical experiments, measuring and processing the corresponding data to obtain channel characteristics. In the case of medical implants, this could be extremely difficult if at all possible. ITL's immersive visualization environment overcomes this barrier. The project

is part of the ITL Pervasive Information Technologies Program. The Web site is http://www.itl.nist.gov/ITLPrograms/Pervasive_Information/index.html.

ITL Usability and Biometric Research Aids Hostage Rescue Efforts

In support of the FBI Hostage Rescue Team, ITL researchers developed a set of user requirements for the migration of the team's mobile biometric device from a ruggedized laptop configuration to a new small form factor emphasizing a handheld device. The FBI hostage rescue team performs a number of law enforcement tactical functions in all environments and under a variety of conditions, and has included operations such as hostage rescue, barricaded subjects, high-risk arrest and warrant service (raids), and dive search.

The goal of the project is to provide a user interface on a small screen that can be used in a time-constrained stressful environment. Little research has been performed on the use of extremely small platforms to collect biometric data, primarily fingerprints, in stressful environments. The hostage rescue team needs a methodology and design approach to define the user requirements for the user interface of a small (3" x 5") screen for their mobile biometrics capture platform, referred to as the Quick Capture Platform (QCP). ITL's usability and biometrics team developed a user interface approach which the FBI is standardizing. They are working with state and local law enforcement to incorporate this new QCP into their work processes. ITL usability experts will continue the project with a high-fidelity design and research on color and appropriate icons for the small screen. The resulting package of products will provide the materials for the FBI to implement a fully functional QCP on the new smaller device. This research is performed under the auspices of the ITL Identity Management Systems Program. The Web site is <http://www.itl.nist.gov/ITLPrograms/IDMS/external/>.

***e-Handbook of Statistical Methods* a Valuable Resource for Scientists and Engineers**

The NIST/SEMATECH *e-Handbook of Statistical Methods* is a valuable online resource designed to help scientists and engineers incorporate statistical methods into their work as efficiently as possible. Consisting of eight chapters, the engineering statistics handbook provides in-depth information on exploratory data analysis, measurement process characterization, production process characterization, process modeling, process improvement, process monitoring and control, product and process comparisons, and assessing product reliability. In addition to guidance, tools, and aids to use the resource, the handbook includes a search feature and a detailed table of contents. The Web site is <http://www.itl.nist.gov/div898/handbook/index.htm>.

UPDATE ON NEW PUBLICATIONS

Recommendation for Applications Using Approved Hash Algorithms

By Quynh Dang

NIST Special Publication 800-107

February 2009

<http://csrc.nist.gov/publications/nistpubs/800-107/NIST-SP-800-107.pdf>

Cryptographic hash functions that compute a fixed-length message digest from arbitrary length messages are widely used for many purposes in information security. This document provides security guidelines for achieving the required or desired security strengths when using cryptographic applications that employ the approved cryptographic hash functions specified in Federal Information Processing Standard (FIPS) 180-3. These include functions such as digital signature applications, Keyed-hash Message Authentication Codes (HMACs), and Hash-based Key Derivation Functions (HKDFs).

Randomized Hashing for Digital Signatures

By Quynh Dang

NIST Special Publication 800-106

February 2009

<http://csrc.nist.gov/publications/nistpubs/800-106/NIST-SP-800-106.pdf>

NIST approved digital signature algorithms require the use of an approved cryptographic hash function in the generation and verification of signatures. Approved cryptographic hash functions and digital signature algorithms can be found in Federal Information Processing Standard (FIPS) 180-3 and FIPS 186-3, respectively. The security provided by the cryptographic hash function is vital to the security of a digital signature application. This Recommendation specifies a method to enhance the security of the cryptographic hash functions used in digital signature applications by randomizing the messages that are signed.

PIV Card Application and Middleware Interface Test Guidelines (SP800-73-2 Compliance)

By Ramaswamy Chandramouli, Hildegard Ferraiolo, Ketan Mehta, and Levent Evuboalu

NIST Special Publication 800-85 A-1

March 2009

<http://csrc.nist.gov/publications/nistpubs/800-85A-1/nist-sp800-85A-1.pdf>

This document provides test requirements and test assertions that could be used to validate the compliance/conformance of two PIV components—*PIV middleware* and *PIV card application* with the specifications in NIST SP 800-73-2. Because NIST SP 800-73-2 specifications were developed for meeting interoperability goals of Federal Information Processing Standard (FIPS) 201, the conformance tests in this document provide the assurance that the set of PIV middleware and PIV card applications that have passed these tests are interoperable. This in turn facilitates marketing and procurement of FIPS 201-conformant products that meet the goals of Homeland Security Presidential Directive-12.

Computer Security Division 2008 Annual Report

Patrick O'Reilly, Editor

NISTIR 7536

March 2009

<http://csrc.nist.gov/publications/PubsNISTIRs.html>

This publication presents the Computer Security Division's Annual Report for FY 2008. The report provides highlights of division activities and projects of FY 2008 and outlines proposed plans for FY 2009.

Slap Fingerprint Segmentation Evaluation II – Procedures and Results

By Craig I. Watson

NISTIR 7553

February 2009

http://fingerprint.nist.gov/slapsegII/SlapSegII_NISTIR_7553.pdf

In 2004, ITL conducted a fingerprint slap segmentation study to assess the state of the art in fingerprint segmentation technology. Given the development of new technology, it became necessary to reassess the current state of the art of segmentation algorithms. SlapSegII gives providers of this technology the opportunity to participate multiple times as their technology improves and compare their results to previous results on a fixed standard database. The SlapSegII testing strategy, evaluation data, and measure of successful segmentation are discussed in detail in this evaluation testing plan.

Complex Systems Program Activities Summary, Fiscal Years 2007-2008

By Sanford P. Ressler

NISTIR 7569

March 2009

<https://nife.nist.gov:8443/publications/viewPubs.do?pubID=901771>

This report summarizes the work of the Complex Systems Program within the Information Technology Laboratory. The report presents background material, an overview of program's activities, strategic goals and objectives, project descriptions, significant technical accomplishments, and future plans for the program.

Fast Iterative Solver for Convection-Diffusion Systems with Spectral Elements

By Paul A. Lott

NISTIR 7574

March 2009

aaron.lott@nist.gov

This report introduces a solver and preconditioning technique based on Domain Decomposition and the Fast Diagonalization Method that can be applied to tensor product-based discretizations of the steady convection-diffusion equation. The method is based on iterative substructuring where fast diagonalization is used to efficiently eliminate the interior degrees of freedom and subsidiary subdomain solves. We demonstrate the effectiveness of this method in numerical simulations using a spectral element discretization.

An Evaluation of Automated Latent Fingerprint Identification Technology (Phase II)

By Michael Indovina, Vladimir Dvornychenko, Elham Tabassi, George W. Quinn, Patrick Grother, Stephen Meagher, and Michael Garris

NISTIR 7577

April 2009

http://fingerprint.nist.gov/latent/NISTIR_7577_ELFT_PhaseII.pdf

NIST, with the cooperation of eight technology providers, performed a test of accuracy for searching latent fingerprints when using automatically extracted features and matching (AFEM). This report provides the design, process, assumptions, limitations, results, observations, and conclusions of Phase II of the Evaluation of Latent Fingerprint Technology (ELFT) project. The test was open to both the commercial and academic communities, and participants included vendors of Automated Fingerprint Identification Systems (AFIS).

MARK YOUR CALENDAR

Safeguarding Health Information: Building Assurance through Effective Security Assessments - A CMS & NIST HIPAA Security Rule Conference

Dates: May 18-19, 2009

Place: NIST, Gaithersburg, Maryland

Sponsors: NIST and the Department of Health and Human Services (HHS) Centers for Medicare and Medicaid Services (CMS) Office of E-Health Standards and Services (OESS)

The conference will focus on challenges, tips, and techniques for implementing the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, with particular focus on strategies for assessing the effectiveness of implemented security controls to support compliance and audit, as well as an organization's overarching risk management program. Topics will include assessment frameworks and methodologies; assessment perspectives from assessors and organizations; trends in security technologies and safeguards, and their applicability to health information technology and the secure exchange of health information. The target audience is HIPAA Security Rule implementers, covered entity security and privacy Officers, audit and assessment teams, and risk executives.

NIST contacts: Kevin Stine, 301/975-8670, kevin.stine@nist.gov

Matthew Scholl, 301/975-941, mscholl@nist.gov

Conference Web site: http://csrc.nist.gov/news_events/HIPAA-May2009_workshop/

Key Management Workshop

Dates: June 8-9, 2009

Location: NIST; Gaithersburg, Maryland

Key management is a fundamental part of cryptographic technology and is considered the most difficult aspect associated with its use. Of particular concern are the scalability of the methods used to distribute keys and the usability of these methods. NIST is undertaking an effort to improve the overall key management strategies used by the public and private sectors in order to enhance usability of cryptographic technology,

provide scalability across all cryptographic technologies, and support a global cryptographic key management infrastructure.

NIST contact: Elaine Barker, 301/975/2911, keymanagementworkshop@nist.gov
Workshop Web site: http://www.csrc.nist.gov/groups/ST/key_mgmt/

Biometric Consortium Conference 2009 (BC2009) and Technology Expo

Dates: September 22-24, 2009

Place: Tampa Convention Center, Tampa, Florida

Sponsors: NIST, National Security Agency, Department of Homeland Security, Department of Defense Biometrics Task Force, National Institute of Justice, General Services Administration Office of Technology Strategy, Department of Transportation Volpe Center, Armed Forces Communications and Electronics Association International

One of the leading Biometric conferences, BC2009 will address the important role that biometrics can play in the identification and verification of individuals in government and commercial applications worldwide. Nearly 2,000 participants will attend, including 100 speakers, 60 federal, state and local agencies, 25 universities, the biometric industry, and users. The two and one-half day program will feature multiple conference sessions, an IEEE Conference on Biometrics, Identity, and Security, and panel discussions and Q&A.

NIST contact: Fernando Podio, 301/975-2947, fernando.podio@nist.gov
Conference Web site: <http://www.biometrics.org/>

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.