Information Technology Laboratory Newsletter

May 2012

Issue 118

ITL GOES GREEN!!

To reduce our carbon footprint, ITL is discontinuing the paper editions of the ITL Newsletter and the ITL Bulletin. If you are not already receiving ITL newsletters and bulletins via email, go to the ITL home page here and sign up in the lower right corner. Our newsletters and bulletins reach more than 5,000 readers electronically. In addition, our information products are always available online on our ITL home page.

ITL Enhances Secure Hash Standard

To allow more flexibility and efficiency in implementing the secure hash algorithms in many computer network applications, ITL proposed a revision to Federal Information Processing Standard (FIPS) 180-3, *Secure Hash Standard (SHS)*. Approved by the Secretary of Commerce and effective March 6, 2012, FIPS 180-4 updates FIPS 180-3 by providing a general procedure for creating an initialization value, adding two additional secure hash algorithms to the standard (SHA-512/224 and SHA-512/256), and removing a restriction that padding must be done before hash computation begins, which was required in FIPS 180-3. Removing the restriction on the padding operation in the secure hash algorithms will potentially permit a more flexible and efficient implementation of the algorithms. The *Federal Register* notice announcing the approval of the new standard is available here. FIPS 180-4 is available here.

NIST Team Receives Supercomputer Time to Study Concrete Flow

A team of researchers from ITL and NIST's Engineering Laboratory (EL) has been awarded 22 million hours of computer time for 2012 from the Department of Energy (DOE) to support the study of the flow properties of large-particle suspensions such as concrete. The award is for the second of a three-year, peer-reviewed proposal to DOE's Innovative and Novel Computational Impact on Theory and Experiment (INCITE) program. High-fidelity flow simulations with many thousands of particles with a wide range of sizes and shapes in a non-Newtonian fluid matrix are enabling the determination of fundamental rheological parameters such as stress and strain rate in non-analytical rheometers and mixing geometries, properties that cannot now be measured accurately in industrial settings. NIST standard reference materials for suspension rheology are also being designed using the results of these simulations.

Not only will this work solve a critical outstanding problem in the cement and concrete industry, but it is expected to have an enormous influence on the wide array of industries that use vane rheometers and mixers such as food processing, water treatment, coatings, and pharmaceuticals. The research team includes William George, Marc Olano, and Judith Terrill of ITL, Nicos Martys and Edward Garboczi of EL, and Pascal Hebraud of CNRS/ESPCI (France). Simulations will be run in the Leadership Computing Facility of Argonne National Laboratory on "Intrepid," an IBM Blue Gene/P system with 164,000 cores, 80 terabytes of RAM, and a peak performance of 557 teraflops. Further information about the INCITE program can be obtained here; details of the most recent award are found here.

ITL's Cloud Computing Program Contributes to International Standards

ISO/IEC JTC1 SC38 Distributed Application Platform & Services newly formed Working Group 3 (WG3) on Cloud Computing held its first meeting February 20-25, 2012, in Vancouver, Canada. As part of its work agenda, WG3 had two new work items for standards development: a Cloud Computing Reference Architecture (RA) and a Cloud Computing Vocabulary. The ITL Cloud Computing program's Reference Architecture and Vocabulary (NIST Special Publication 500-292) were submitted to the U.S. National Body (DAPS 38) where it became the core document for the U.S. submission to WG3. During the WG3 meeting, the U.S. contributions on both the RA and Vocabulary were accepted as the base documents from which the WG will proceed in its work. That the NIST Cloud Computing Reference Architecture and Vocabulary were recognized and accepted as the starting point for the international standardization effort reflects the impact and importance of ITL's Cloud Computing program efforts. See here.

Mobile Device Security

The technological advances embodied in today's Smart Phones have introduced significant changes and challenges to the way we communicate and conduct our everyday lives. Commercial Smart Phones have become a "must-have" electronic gadget for people of all ages, but also an indispensable tool for enterprise operations. These Smart Phones are replacing the need for laptops and desktops with processor speeds surpassing 1GHz, storage capacity exceeding 32GB, support for numerous cellular and wireless networking technologies, and countless applications available for instant download. In order to capitalize on these advances, significant obstacles need to be overcome to mitigate the new risks presented by the use of commercial off-the-shelf (COTS) Smart Phones. These new risks must be well-understood and mitigated by a combination of operational, management and technical controls before a mobile workforce can take full advantage of these new capabilities.

ITL and the White House Communications Agency cosponsored a Mobile Device Security Technical Exchange Meeting on January, 24, 2012, at NIST. The meeting shared lessons learned from pilot Smart Phone deployments, fostered collaboration among government agencies, addressed interoperability issues, and provided a forum for the exchange of technical information. Speakers from the Defense Advanced Research Projects Agency (DARPA), the National Security Agency (NSA), the Department of Defense (DoD), and the Federal Communications Commission (FCC) discussed open problems and technology gaps that need to be addressed by industry and government agencies. The event was attended by over 200 government employees representing NSA, DoD, FCC, Defense Information Systems Agency, Department of Treasury, Department of State, Department of Justice, Department of Energy, Department of Homeland Security, Federal Trade Commission, the U.S. General Services Administration, and the Federal Bureau of Investigation.

© Nicholas McIntosh

Proposed Change to Federal Information Processing Standard (FIPS) 186-3, Digital Signature Standard (DSS)

ITL is requesting comments on proposed changes to FIPS 186-3, *Digital Signature Standard (DSS)*. The *Federal Register* notice of April 10, 2012, requested that electronic comments be sent by **May 25, 2012,** here , with 186-3 Change Notice in the subject line. The proposed revisions are available here. The *Federal Register* notice is available here.

Selected New Publications

Specification for WS-Biometric Devices (WS-BD), Version 1
By Ross Michaels, Kevin Mangold, Matthew Aronoff, Kayee Kwong, and Karen Marshall
NIST Special Publication 500-288
March 2012

Web Services-Biometric Devices is a specification describing how to expose a biometric sensor to various clients via web services. By using Web services as a means for interoperability, the capabilities and reach of biometrics is significantly improved.

Guidelines for Securing Wireless Local Area Networks (WLANs)
By Murugiah Souppaya and Karen Scarfone
NIST Special Publication 800-153
February 2012

A *wireless local area network (WLAN)* is a group of wireless networking devices within a limited geographic area, such as an office building, that exchange data through radio communications. The security of each WLAN is heavily dependent on how well each WLAN component—including client devices, access points (APs), and wireless switches—is secured throughout the WLAN life cycle. This publication helps organizations to improve their WLAN security by providing recommendations for WLAN security configuration and monitoring.

Recommendation for Random Number Generation Using Deterministic Random Bit Generators
By Elaine Barker and John Kelsey
NIST Special Publication 800-90A
January 2012

This Recommendation specifies mechanisms for the generation of random bits using deterministic methods. The methods provided are based on either hash functions, block cipher algorithms, or number theoretic problems.

Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
By William C. Barker and Elaine Barker
NIST Special Publication 800-67, Rev. 1
January 2012

This publication specifies the Triple Data Encryption Algorithm (TDEA), including its primary component cryptographic engine, the Data Encryption Algorithm (DEA). When implemented in an SP 800-38 series-compliant mode of operation and in a FIPS 140-2-compliant cryptographic module, TDEA may be used by federal organizations to protect sensitive unclassified data.
This recommendation defines the mathematical steps required to cryptographically protect data using TDEA and to subsequently process such protected data.

Technical Evaluation, Testing and Validation of the Usability of Electronic Health Records
By Svetlana Z. Lowry, Matthew T. Quinn, Mala Ramaiah, Robert M. Schumacher, Emily S. Patterson, Robert North, Jiajie Zhang, Michael C. Gibbons, and Patricia Abbott
NISTIR 7804
February 2012

This document summarizes the rationale for an Electronic Health Record (EHR) Usability Protocol (EUP) and outlines procedures for design evaluation and human user performance testing of EHR systems. The procedures include general steps and guidance for evaluating an EHR user interface from clinical and human factors perspectives, and for conducting a validation study (i.e., summative usability test) of EHR user interfaces with representative user groups performing realistic tasks.

IREX III – Performance of Iris Identification Algorithms
By Patrick Grother, George Quinn, J.R. Matey, M. Ngan, Wayne Salamon, G. Fiumara, and Craig Watson
NISTIR 7836
April 2012

Iris recognition has long been held as an accurate and fast biometric. In the first public evaluation of one-to-many iris identification technologies, this third activity in the Iris Exchange (IREX) program measured the core algorithmic efficacy and duration of the core processing functions of 92 algorithms from 11 implementing organizations operating on nearly 6 million images of 4 million eyes of 2 million people. As such, this report documents the state of the art of iris recognition technology operating on archival imagery, demonstrates the existence of a large and diverse range of implementations beyond those described in the academic literature, and identifies factors contributing to recognition failure.

Upcoming Technical Conferences

Technical Aspects of Botnets Workshop

Date: May 30, 2012
Place: NIST, Gaithersburg, Maryland
Audience: Industry, government, and academia

While security risks on the Internet continue to exist in many areas, one increasingly exploited threat is the global rise of botnets. A botnet infection can lead to the monitoring of a consumer's personal information and communication, and exploitation of that consumer's computing power and Internet access. This workshop seeks to engage all stakeholders to identify the available and needed technologies and tools to recognize, prevent, and remediate botnets; explore current and future efforts to develop botnet metrics and methodologies for measuring and reporting botnet metrics over time; and understand where ecosystem stakeholders are in terms of roles and responsibilities.

NIST contacts: Jon Boyens, (301) 975-3449, jon.boyens@nist.gov
Celia Paulsen, (301) 975-5981, celia.paulsen@nist.gov

Cloud Computing Forum & Workshop V

Dates: June 5-7, 2012
Place: Department of Commerce, Washington, D.C.
Audience: Industry, government, and academia

The purpose of the forum and workshop is to show federal leadership and support for the NIST technology role in U.S. government agency adoption of cloud computing to reduce costs and improve services and to strengthen relationships with the private sector. The event will calibrate the NIST Cloud Computing program and the USG Cloud Computing Technology Roadmap initiative with external stakeholders. Panels focusing on federal and private sector topics of interest and showcases work completed through NIST-chaired public working groups will be featured.

NIST contact: Robert Bohn, (301) 975-4731, robert.bohn@nist.gov

Safeguarding Health Information: Building Assurance through HIPAA Security

Dates: June 6-7, 2012
Place: Ronald Reagan Building, Washington, D.C.
Audience: Industry, government, and healthcare providers
Sponsors: NIST, HHS Office for Civil Rights
Cost: $395 for in-person attendees and webcast attendees

The conference will explore the current health information technology security landscape and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. The event will highlight the present state of health information security, and practical strategies, tips and techniques for implementing the HIPAA Security Rule. The Security Rule sets federal standards to protect the confidentiality, integrity, and availability of electronic protected health information by requiring HIPAA covered entities and their business associates to implement and maintain administrative, physical, and technical safeguards.

NIST contact: Kevin Stine, (301) 975-4483, kevin.stine@nist.gov

NIST – Bell Labs Workshop on Large-Scale Complex Networks

Date: June 8, 2012
Place: NIST, Gaithersburg, Maryland
Audience: Industry, government, and academia
Sponsors: NIST and Alcatel-Lucent, Bell Labs

The 2nd NIST - Bell Labs Workshop will highlight and discuss current and emerging research on large-scale geometry of complex networks, including hyperbolicity and its possible impact on network performance, reliability, robustness, and security; processes on said complex networks, including percolation and diffusion; and interplay between processes on networks and network evolution.

Participation to the workshop is via invitation. If you would like to attend, please contact Vladimir Marbukh, (301) 975-2235, vladimir.marbukh@nist.gov

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 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
Email: elizabeth.lennon@nist.gov

TO SUBSCRIBE TO THE ELECTRONIC EDITION OF THE ITL NEWSLETTER, GO TO ITL HOMEPAGE

Many deer find a home on the NIST Campus in Gaithersburg, MD.