

Information Technology Laboratory Newsletter

INSIDE THIS ISSUE

Cloud Computing and Big Data Communities Join Forces for Progress

Expansion of ITL's Biometric Data Exchange Standard

Searchable Catalog of Computer Forensic Tools

Cybersecurity Framework

NIST Team Awarded 30M Hours of Supercomputer Time to Study Properties of Dense Suspensions

Selected New Publications

Upcoming Technical Conferences



Credit: Shutterstock

March—April 2013

Issue 122

Cloud Computing and Big Data Communities Join Forces for Progress

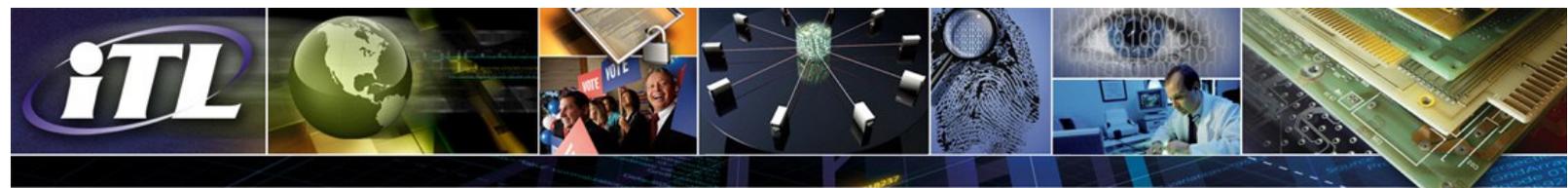
More than 900 U.S. and international participants and a webcast audience of more than 2400 views came together at the recent NIST Joint Cloud and Big Data Forum to explore the opportunities created by the intersection of these exciting new technologies. Emerging from the forum was a consensus that cloud computing environments – networked computing resources available on demand – make big data solutions – those that use massive data sets to go beyond conventional discovery methods – more powerful and more accessible.

The ability to gather, process, and use “big data” will change our understanding of and how we interact with our world. In the words of NIST Director Pat Gallagher: “We are really looking at a new paradigm, a place of data primacy, where everything starts with the consideration of the data rather than consideration of the technology.” With massive data becoming ubiquitous, the need for IT systems that support the processing and management of these datasets becomes more important.

The answer to the question of whether cloud computing technology can provide the functionality and performance to meet the requirements of these big data systems seems to be a resounding “yes.” As Federal CIO Steven VanRoekel said during his keynote address: “The combination of cloud and big data not only can create useful insights, but also can create incredible value.”

Many challenges remain to create successful big data and cloud computing systems. During the workshop, progress was made understanding what big data is, what the system requirements are to support big data, and how cloud computing will need to adapt to meet these requirements. A good example of this is the need for cloud-to-cloud interoperability. Vint Cerf, Chief Internet Evangelist at Google, said: “In the future, there will be special capabilities in some clouds that others don’t offer.” For example, partial calculations completed in one cloud may need to be moved directly to another better suited for the next step. This requires seamless portability between clouds while preserving integrity, access control, and privacy of data across these transitions.

Additional progress was made during working sessions covering such topics as standards, security, metrics, definitions, and collaborations, and NIST will continue this progress in working groups and workshops on cloud computing and big data in the coming year. The [webcast](#) of the workshop is available.



Expansion of ITL's Biometric Data Exchange Standard



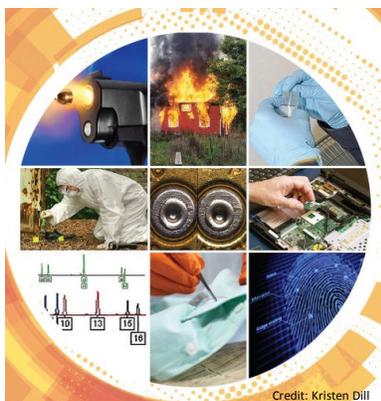
ITL researchers are collaborating with biometrics and forensics experts worldwide to expand the ANSI/NIST-ITL standard: "Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information." The standard is widely used by domestic and international law enforcement agencies for the exchange of forensics and biometrics information.

More than 150 representatives from federal, state, and local government agencies, foreign governments, international organizations (such as INTERPOL), academia, and private industry, met recently at NIST to address proposed additions and revisions to the standard. The workshop focused primarily on forensics applications and mobile biometrics. ITL presented a proposal to establish a database for the analysis of ballistic information, in order to develop and test automated matching algorithms. The proposal was enthusiastically received, and requests were made to expand the concept to cover all 'toolmarks' (such as tiretracks, shoeprints, etc.). The approach is similar to that done successfully by ITL for several years for fingerprint, facial image, and iris data. In addition, a working group was established to develop a new Best Practice Recommendations document on mobile biometric applications.

A supplement to the standard will be submitted to canvassers for voting in the early summer of 2013. More information about the [standard](#).

Searchable Catalog of Computer Forensics Tools

ITL has developed a catalog of computer forensics tools. The catalog provides an easily searchable resource of forensics tools for practitioners to find tools that meet their specific technical needs. The catalog affords the ability to search by technical parameters based on specific computer forensics functions, such as disk imaging or deleted file recovery. The catalog also presents a picture of the computer forensics tool landscape, showing where there are gaps, i.e., functions for which there are no tools. Tool information is provided by the vendor. The [catalog](#) is a partnership between NIST's Information Technology



Laboratory and Office of Law Enforcement Standards, and the Department of Homeland Security, Science & Technology Directorate, Cyber Security Division.

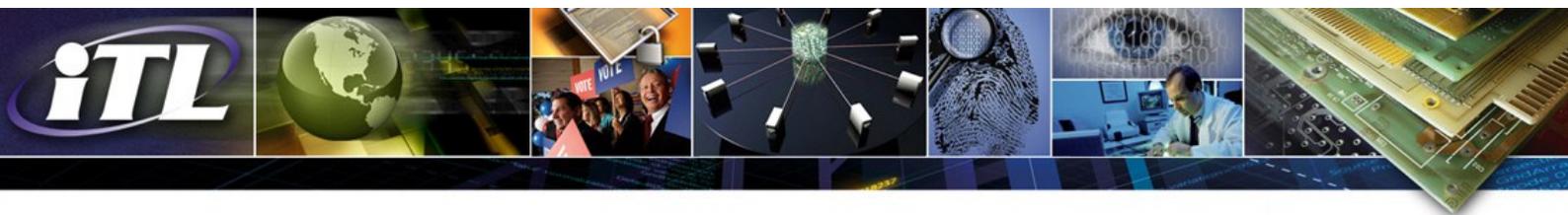
Cybersecurity Framework

Under the Executive Order *Improving Critical Infrastructure Cybersecurity*, the President has directed NIST to work with stakeholders to develop a voluntary [framework](#) for reducing cyber risks to critical infrastructure. The framework will consist of standards, guidelines, and best practices to strengthen the protection of information systems supporting critical infrastructure operations. It will promote the wide adoption of practices to increase cybersecurity across all sectors and industry types. ITL will host a workshop on April 3, 2013, to describe progress to date (see Upcoming Technical Conferences).

NIST Team Awarded 30M Hours of Supercomputer Time to Study Properties of Dense Suspensions

The Department of Energy (DOE) awarded a team of researchers from NIST's Information Technology Laboratory and Engineering Laboratory (EL) 30 million hours of supercomputer time for calendar year 2013 to support the study of the flow properties of large-particle dense suspensions such as concrete. The award is for the third of a three-year, peer-reviewed proposal to DOE's Innovative and Novel Computational Impact on Theory and Experiment (INCITE) program. Highly detailed simulations of suspensions, comprising many thousands of particles with a wide range of sizes and shapes suspended in a non-Newtonian fluid matrix, are enhancing the understanding of fundamental rheological properties such as viscosity versus strain rate, in non-analytical rheometer and mixing geometries. These properties currently cannot be measured accurately in industrial settings. The results of these simulations are also being used in the design of NIST standard reference materials for suspension rheology.

Not only will this work solve a critical outstanding problem in the cement and concrete industry, but it will also 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, Steven Satterfield, 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 and on their newest machine Mira, an IBM Blue Gene/Q, which is currently number 3 in the "Top 500" list of supercomputer installations.



Selected New Publications

[Report on the Static Analysis Tool Exposition \(SATE\) IV](#)

By Vadim Okun, Aurelien Delaitre, and Paul Black

NIST Special Publication 500-297
January 2013

The NIST SAMATE project conducted the fourth Static Analysis Tool Exposition (SATE IV) to advance research in static analysis tools that find security defects in source code. The main goals of SATE were to enable empirical research based on large test sets and to encourage improvement and speed adoption of tools. Participating tool makers ran their tool on a set of programs, and ITL researchers performed a partial analysis of tool reports. Results were presented at the SATE IV Workshop in March 2012. This paper describes the SATE procedures and provides observations on the data collected.

[The Twenty-First Text REtrieval Conference Proceedings \(TREC 2012\)](#)

Ellen M. Voorhees and Lori M. Buckland, Editors
NIST Special Publication 500-298
February 2013

This report constitutes the proceedings of the Twenty-First Text REtrieval Conference (TREC 2012) held in Gaithersburg, Maryland, on November 6-9, 2012. The conference was cosponsored by the National Institute of Standards and Technology (NIST), the Defense Advanced Research Projects Agency (DARPA), and the Advanced Research and Development Activity (ARDA).

[Security Content Automation Protocol \(SCAP\) Version 1.2 Validation Program Test Requirements](#)

By John Banghart, Melanie Cook, Stephen Quinn, David Waltermire, and Andrew Bove
NISTIR 7511 Revision 3
February 2013

This report defines the requirements and associated test procedures necessary for products to achieve one or more Security Content Automation Protocol (SCAP) validations. Validation is awarded based on a defined set of SCAP capabilities by independent laboratories that have been accredited for SCAP testing by the NIST National Voluntary Laboratory Accreditation Program (NVLAP).

[Examination of Downsampling Strategies for Converting 1000 ppi Fingerprint Imagery to 500 ppi](#)

By Shahram Orandi, John M. Libert, John D. Grantham, Margaret Lepley, Bruce Bandini, Kenneth Ko, Lindsay M. Petersen, Stephen S. Wood, and Stephen G. Harvey
NISTIR 7839
January 2013

Currently the bulk of fingerprint data in operations is captured, processed and stored at 500 ppi using the WSQ compressed digital format. With the transition to 1000 ppi, some systems will unavoidably contain an overlap between 500 ppi and 1000 ppi operational pathways. This overlap may be a result of legacy infrastructure limitations, or some other financial or logistical reason. Additionally, there will still be a need to compare newly

collected 1000 ppi images against legacy 500 ppi images, for both one-to-one and one-to-many scenarios. To create a bridge between legacy and modern data, there needs to be a pathway for interoperability of legacy and modern data on equal footing by converting one of the images to the same resolution as the other. Downsampling of the higher resolution 1000 ppi imagery to 500 ppi provides this pathway. The study compares several computational methods for downsampling of modern fingerprint images from 1000 ppi to 500 ppi.

[Alternative Methods of Latent Fingerprint Enhancement and Metrics for Comparing Them](#)

By Alfred S. Carasso
NISTIR 7910
January 2013

Digital enhancement of latent fingerprints using Photoshop processing is the preferred methodology among law enforcement forensic experts. This report explores alternative enhancement methods that are independent of Photoshop, relying instead on such widely used scientific image analysis packages as MATLAB, IDL, and PV-WAVE. In addition, standard image metrics are applied to the processed images and shown capable of distinguishing among various types of enhancements. The discussion is anchored around three illustrative examples, consisting of 8-bit greyscale latent fingerprint image pairs, extracted from the NIST forensic database. It is shown that alternative enhancement methods exist that can recover potentially significant fine-scale information, such as may elude standard forensic Photoshop processing.

[Proceedings of the Cybersecurity in Cyber-Physical Systems Workshop, April 23-24, 2012](#)

Tanya Brewer, Editor
NISTIR 7916
February 2013

This document constitutes the proceedings of the Cybersecurity in Cyber-Physical Workshop, April 23 – 24, 2012, complete with abstracts and slides from presenters. Some of the cyber-physical systems covered during the first day of the workshop included networked automotive vehicles, networked medical devices, semiconductor manufacturing, and cyber-physical testbeds. Day two of the workshop covered the electric Smart Grid.

[Summary of the Workshop on Cryptographic Key Management Systems \(CKMS\)](#)

By Elaine B. Barker, Miles Smid, and Dennis Branstad
January 2103

This document provides a summary of the workshop held on September 10-11, 2012, to discuss two documents that were posted for public comment: SP 800-130, *A Framework for Designing Cryptographic Key Management Systems*, and a table of proposed requirements for SP 800-152, *A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)*. In addition, the workshop included discussions on the hard problems associated with key management.



Upcoming Technical Conferences

[26th Annual Federal Information System Security](#)

[Education Association \(FISSEA\) Conference](#)

Dates and Place: March 19-21, 2013, at NIST

Sponsors: NIST and FISSEA

Cost: \$170

The conference theme is "Making Connections in Cybersecurity and Information Security Education." 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/conducting training; an update on the National Initiative for Cybersecurity Education (NICE); networking opportunities; professional development; and an opportunity to meet industry partners at vendor exhibit.

NIST contacts: Patricia Toth, patricia.toth@nist.gov, and Peggy Himes, peggy.himes@nist.gov

[Accessible Voting Technology Research Workshop](#)

Dates and Place: April 1-2, 2013, at NIST

Sponsors: NIST and the U.S. Election Assistance Commission

Cost: None

This workshop will explore current and future research in accessible voting technology. Topics will include innovative assistive applications and techniques; new approaches to accessibility in voting; accessibility research benchmarks and results; transitioning research to industry; new and existing devices that provide accessible access to elements of the voting process; and challenges in accessible voting.

NIST contact: Sharon Laskowski, sharon.laskowski@nist.gov

[Cybersecurity Framework](#)

Date and Place: April 3, 2013, at NIST

Sponsor: NIST

Cost: None

NIST has been tasked, under Executive Order 13636, to develop a cybersecurity framework to mitigate cybersecurity risks for the nation's critical infrastructure. This workshop will report on progress to date.

NIST contact: Suzanne Lightman, suzanne.lightman@nist.gov

[Designed-in Cybersecurity for Cyber-Physical Systems](#)

Dates and Place: April 4-5, 2013, at NIST

Sponsors: NIST and the Cyber Security Research Alliance (CSRA)

Cost: \$95

This conference will explore emerging research needs for cybersecurity in cyber-physical systems (CPS) with the diverse cyber-physical community at large. Topics will include security in acquisition and implementation, getting reliable information on vulnerabilities and threats, securing the base, supply chain impact, approaches to assurance for CPS, and enabling trustworthy operation readiness.

NIST contact: Suzanne Lightman, suzanne.lightman@nist.gov

[Workshop on Improving Trust in the Online Marketplace](#)

Dates and Place: April 10-11, 2013, at NIST

Sponsor: NIST

Cost: \$104

This workshop will focus on technical and administrative efforts to increase trust online by improving the Public Key Infrastructure (PKI) certificate marketplace supporting Secure Socket Layer (SSL) and Transport Layer Security (TLS). Recent attacks against individuals and companies online have utilized known vulnerabilities in certificate management in order to spoof websites or gain trust to install malicious software without the user's knowledge. The workshop will provide an opportunity for industry, research and academia communities, and government sectors to review, promote, and move toward consensus on emerging industry standards and guidelines and to learn about NIST's current cryptographic research, activities, programs and standards development.

NIST contact: Andrew Regenscheid,

andrew.regenscheid@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). 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](#)