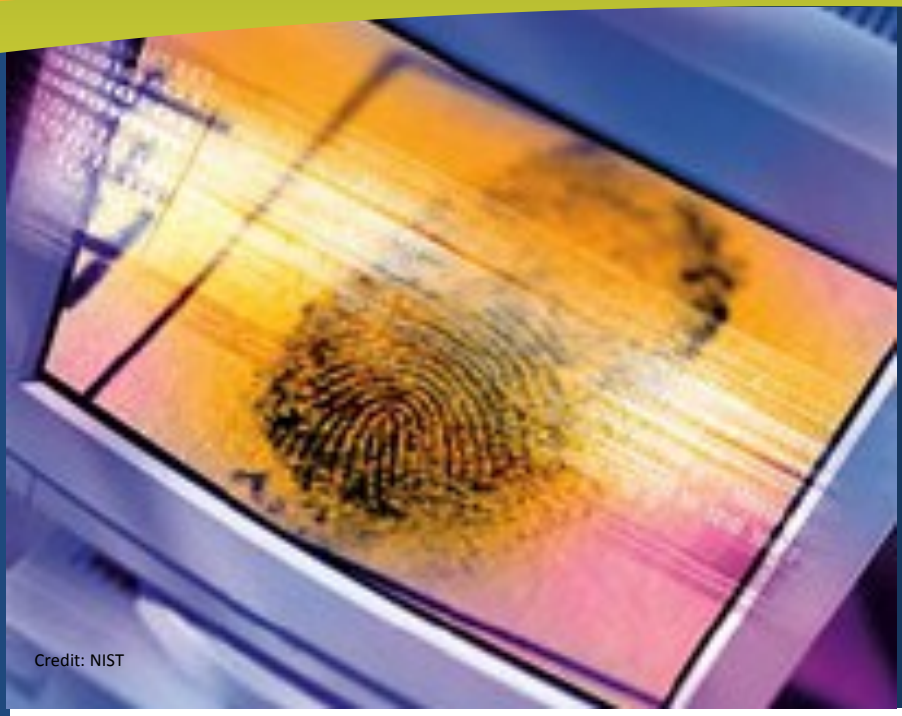
Information Technology Laboratory Newsletter


Credit: NIST

May—June 2013

Issue 123

INSIDE THIS ISSUE

ITL Forensics Program Provides Infrastructure for U.S. Law Enforcement

Forensic science provides one of the basic structural elements of the U.S. criminal justice system. It provides the methodologies for understanding crime scenes, analyzing evidence, identifying suspects, and prosecuting and convicting criminals while exonerating innocent people. The ITL Forensics Program advances the measurements and standards infrastructure for forensic science through the application of computer science, mathematics, and statistics.

The program goals include improving the accuracy, reliability, and scientific validity of forensic science as well as enhancing the technology, usability, and interoperability of forensic systems and methods. In the area of human identity, we are developing metrics and standards to accelerate development of technologies that analyze latent fingerprints, face images, and voice. These technologies will aid forensic examiners in identifying potential suspects. We are enhancing interoperability of forensic systems through interface standards that include, in addition to the above evidence, DNA, scars, marks, tattoos, bite marks, and dental records. We are also supporting the development and interoperability of operational fingerprint analysis and matching systems.

In the area of computer forensics, our research results in methodologies to test and verify the operation and output of automated programs that examine computers, including cell phones and other mobile devices, for evidence. We also provide a repository of known software, file profiles, and file signatures that are used by law enforcement and other investigators to determine the identity of files they recover. This repository is called the National Software Reference Library and is distributed as NIST Special Database 28.

In the area of image/video technologies, we are applying metrics and testing methodologies to advance technologies that detect and recognize events in video surveillance data, as well as search for specific persons, objects, or places in such data. These technologies will aid forensic examiners who analyze images and video.

Finally, our statisticians contribute to forensics work at NIST. Examples include activities in statistical science that provide uncertainty analysis for ballistic fingerprinting, for seized drug analysis, and for limits of detection for the presence of drugs. See the ITL Forensics Program website.

ITL Researches Accessible Voting Technology

ITL research in accessible voting systems focuses on identifying and developing technological and administrative solutions that help ensure that all citizens, including those with disabilities, can vote privately and independently, a requirement of the Help America Vote Act (HAVA) of 2002. The goal is to increase the accessibility of new, existing, and emerging technological solutions in such areas as assistive technologies, interoperability, and design of voting systems.

To explore challenges and solutions in accessible voting technology, ITL and the U.S. Election Assistance Commission recently cosponsored a two-day workshop at NIST. The event brought together over 60 participants and a webcast audience of diverse stakeholders, including researchers, election officials, government officials, and voting system manufacturers. Workshop discussion topics included challenges in accessible voting; innovative assistive applications and techniques; new approaches to accessibility in voting; accessibility research benchmarks and results; transitioning research to industry; and new and existing devices that provide accessible access to elements of the voting process.

The outcomes of the workshop will contribute to the planning of the conference Future of Voting Symposium – The People, The Process, The Technology, which will be held later this year. An archive of the webcast, as well as the presentations and posters presented at the workshop are available on the workshop website.

ITL Conducts Course in Measurement Uncertainty and Statistical Analysis for Metrologists from Central and South America

Antonio Possolo, Chief, Statistical Engineering Division, recently taught a four-day course and workshop on the evaluation of measurement uncertainty, and on the statistical analysis of results from interlaboratory studies and proficiency tests, at the "Laboratorio Tecnológico del Uruguay" (LATU, Montevideo, Uruguay). The course benefitted metrologists from the regional metrological organization for the Americas, "Sistema Interamericano de Metrologia (SIM)." The 19 course participants came from Argentina, Brazil, Chile, Costa Rica, Ecuador, Peru, and Uruguay.

ITL Hosts Federal Information Systems Security Educators' Association (FISSEA) Conference

Founded in 1987, FISSEA is an organization run by and for information systems security professionals to assist federal agencies in meeting their information systems security awareness, training, education, and certification responsibilities. ITL recently hosted the 26th annual FISSEA Conference at NIST. Approximately 140 information systems security professionals and trainers attended from federal agencies, industry, and academia. This year's theme was "Making Connections in Cybersecurity and Information Security Education." Attendees learned about new techniques for developing and conducting training, cost-effective practices, workforce development, free resources and contacts, as well as National Initiative for Cybersecurity Education (NICE) activities.

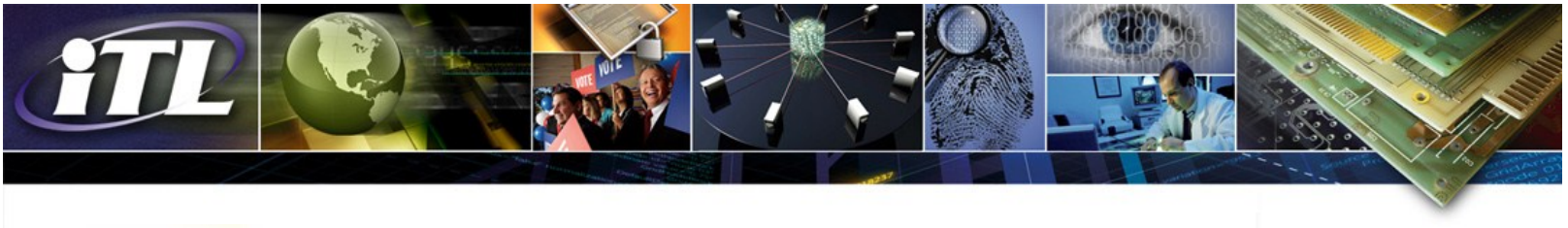
The FISSEA conference continues to be a valuable forum for individuals who are involved with information systems/ cybersecurity workforce development, to learn of ongoing and planned training and education programs and initiatives. The event affords ITL the opportunity to provide assistance to federal agencies as they work to meet their Federal Information Security Management Act (FISMA) responsibilities. For more information, see the FISSEA website.

ITL Staffers Win 2013 Federal 100 Awards

Federal Computer Week recognized three ITL staffers with Federal 100 Awards:

- Jon Boyens, Senior IT Security Specialist, was honored for his leadership of a team that developed a set of standardized, repeatable practices to help federal agencies manage risks to their information and communications technology supply chain in the face of rapid technological evolution.
- Jeremy Grant, Senior Executive Advisor for Identity Management, was recognized for establishing and directing the National Strategy for Trusted Identities in Cyberspace (NSTIC) National Program Office at NIST.
- Adam Sedgewick, Senior IT Policy Advisor, received the award for his role as senior advisor to the CIO Council, providing invaluable behind-the-scenes management, coordination, and operational support for the council's agenda and activities.

The Federal 100 Awards recognize government and industry leaders who have played pivotal roles in the government IT community. The awards were presented on March 20, 2013, at the 24th Annual Federal 100 Awards Gala at the Grand Hyatt Hotel in Washington, D.C.



Selected New Publications

Security and Privacy Controls for Federal Information Systems and Organizations
By the Joint Task Force Transformation Initiative
NIST Special Publication 800-53, Revision 4
April 2013
(Link to be provided)

This publication provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors (both intentional and unintentional). The security and privacy controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk.

The controls address a diverse set of security and privacy requirements across the federal government and critical infrastructure, derived from legislation, Executive Orders, policies, directives, regulations, standards, and/or mission/ business needs. The publication also describes how to develop specialized sets of controls, or overlays, tailored for specific types of missions/business functions, technologies, or environments of operation. Finally, the catalog of security controls addresses security from both a functionality perspective (the strength of security functions and mechanisms provided) and an assurance perspective (the measures of confidence in the implemented security capability). Addressing both security functionality and security assurance ensures that information technology products and the information systems built from those products using sound systems and security engineering principles are sufficiently trustworthy.

Report on the Metrics and Standards for Software Testing (MaSST) Workshop 2012
By Paul E. Black and Elizabeth N. Fong
NISTIR 7920
March 2013

The NIST Software Assurance Metrics And Tool Evaluation (SAMATE) project conducted a workshop on Metrics and Standards for Software Testing (MaSST) on June 20, 2012. The workshop was co-located with the IEEE Sixth International Conference on Software Security and Reliability (SERE) 2012 at NIST. The goals of MaSST were to bring together researchers and practitioners to (1) understand the state of the art and state of practice in software testing; (2) map work needed for improved methods and tools for software testing; and (3) list any important problems needing to be solved. This report contains observations and recommendations based upon the workshop, and includes position statements submitted to the workshop and presentation slides. Presentations addressed software testing standards, best practices in testing, testing techniques, such as fuzzing, model-based, static and dynamic verification, and vulnerability reporting.

Camera Recognition
By Michelle Steves, Brian Stanton, Mary Theofanos, Dana Chisnell, and Hannah Wald
NISTIR 7921
March 2013

The Department of Homeland Security's (DHS) United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program is a biometrically-enhanced identification system primarily situated at border points of entry such as airports and seaports. In a 2004 assessment of the quality of facial images captured by US-VISIT, NIST discovered a widespread problem: many subjects were 1) not directly facing the camera, and 2) had a pose angle of greater than 10 degrees. The findings of NIST's subsequent follow-up studies suggest that the camera used to capture facial images of travelers should look as much as possible like a traditional camera. Knowing where to look will help the subjects being photographed orient themselves in such a way that they are frontal to the camera, thus improving picture quality. This study explored whether participants could discern image capture devices (i.e., cameras) from other types of technology, and the attributes they relied upon to make that distinction.

Configuration of profiling tools for C/C++ applications under 64-bit Linux
By David W. Flater
NIST Technical Note 1790
March 2013

Application profiling tools are the instruments used to measure software performance at the function and application levels. Without careful configuration of the tools and the environment, invalid results are readily obtained. The errors may not become obvious if a large, complex application is profiled before more simple validations are attempted. A set of four simple synthetic reference applications was used to validate configurations for profiling under x86 64 Linux. Results from one validated configuration and examples of observed invalid results are presented. While validation results for specific versions of software quickly lose value, this exercise demonstrates how future configurations can be validated and shows the kinds of errors that may reoccur.

Upcoming Technical Conferences

NIST Exhibits at FOSE 2013
Dates and Place: May 14-16, 2013, at the Walter E. Washington Convention Center, Washington, D.C.
Booth 805

FOSE is the nation's premier event for government technology professionals who need tools, resources, and best practices to transition to the cloud, mitigate cybersecurity threats, and achieve the goals of the Digital Government Strategy (DGS) while managing uncertainty and the critical need to make it all happen on-time and on-budget.
NIST contact: Elizabeth Lennon, elizabeth.lennon@nist.gov

Safeguarding Health Information: Building Assurance through HIPPA Security 2013
Dates and Place: May 21-22, 2013 at the Ronald Reagan Building and International Trade Center, Washington, D.C.
Sponsors: NIST and the Department of Health and Human Services Office of Civil Rights
Cost: $400

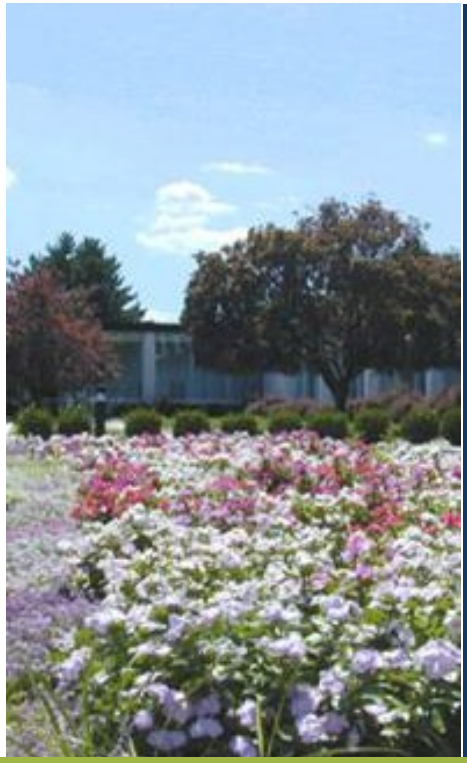
This sixth annual conference will explore the current health information technology security landscape and will give practical tips, techniques, and strategies for implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. The Security Rule sets federal standards to protect 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. Sessions will explore security management and technical assurance of electronic health information. Presentations will cover a variety of current topics including updates on the Omnibus HIPAA/HITECH Final Rule, identity management, strengthening cybersecurity in the healthcare sector, integrating security safeguards into health IT, managing insider threats, securing mobile devices, and more.
NIST contact: Kevin Stine, kevin.stine@nist.gov

2nd Cybersecurity Framework Workshop
Dates and Place: May 29-31, 2013, at Carnegie Mellon University, Pittsburgh, Pennsylvania
Sponsor: NIST
Cost: None

Under Executive Order 13636, NIST was given responsibility to develop a cybersecurity framework to reduce cybersecurity risks for critical infrastructure. This meeting will bring together stakeholders to solicit their comments in person. NIST is interested in collecting information about current risk management practices; use of frameworks, standards, guidelines and best practices; and specific industry practices.
NIST contact: Suzanne Lightman, suzanne.lightman@nist.gov

2013 Biometric Consortium Conference & Biometric Technology Expo
Dates and Place: September 17-19, 2013, Tampa Convention Center, Tampa, Florida
Sponsors: NIST, National Security Agency, and AFCEA International
Cost: $595 - $695

The Biometric Consortium Conference will focus on biometric technologies for defense, homeland security, identity management, border crossing, and electronic commerce. The conference will feature four tracks, including the AFCEA Identity Management (IdM) track, panel discussions, workshops, and a biometrics tutorial. The keynoter will be Jeremy Grant, Senior Executive Advisor for Identity Management, National Strategy for Trusted Identities in Cyberspace (NSTIC), Information Technology Laboratory, NIST.
NIST contact: Fernando Podio, fernando.podio@nist.gov



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

To subscribe to the electronic edition of the ITL Newsletter, go to ITL homepage

The NIST campus in Gaithersburg, Maryland.

Credit: NIST