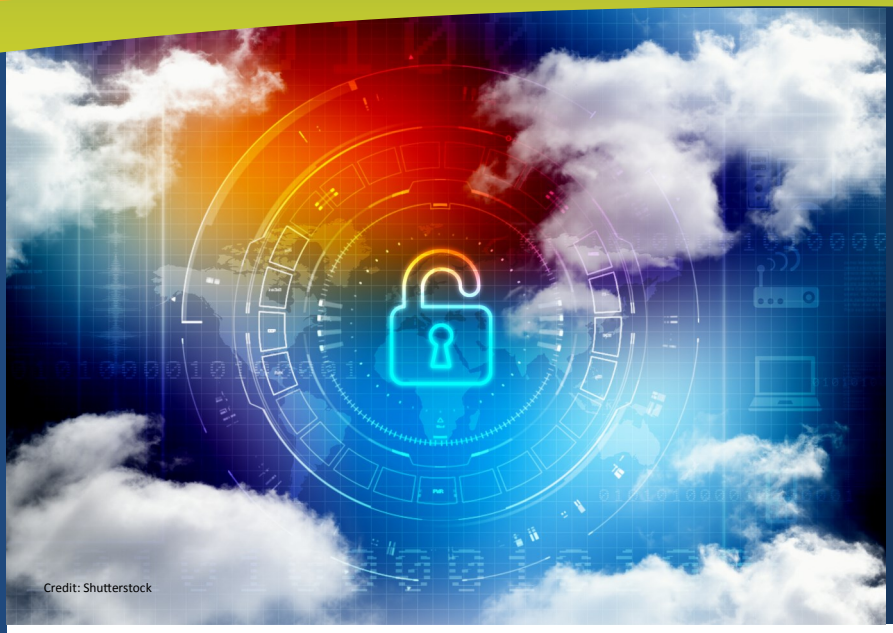
Information Technology Laboratory Newsletter



November—December 2015

Issue 138

INSIDE THIS ISSUE

ITL Focuses on Cyber Supply Chain Risk Management

Federal agencies are concerned about the risks associated with information and communications technology (ICT) products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the ICT supply chain. These risks increase as agencies have less understanding and control over how the technology that they acquire is developed, integrated and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services.

ITL researchers are working with industry partners to identify best practices for managing cyber risks in the supply chain. As an extension of this work, ITL recently hosted a Cyber Supply Chain Risk Management Workshop, which was attended by about 220 representatives from industry and government. Linda Conrad, Head of Strategic Business Risk for Zurich Insurance Group, presented a keynote address discussing cyber supply chain risks and statistics on impacts. Three panels with organizations such as Johnson & Johnson, Intel, John Deere, Cisco, the Edison Electric Institute, the National Electrical Manufacturers Association, and others discussed the cyber supply chain risk environment; the tools, technologies, and processes they use to manage cyber supply chain risk; and relevant standards, guidelines, and acquisition criteria.

Conference attendees participated in an effort to identify and map existing or developing standards which may apply. During breakout sessions, attendees organized into four groups to discuss common risk management tools and techniques used in various industry sectors and organizational strategies including techniques for supplier selection. Several common themes from the discussions emerged, including how to leverage existing organizational structures, utilizing progressive levels of trust, conducting supplier site visits, the need for a common language and taxonomy, sharing of resources between businesses, and awareness and training.

ITL will continue its research on industry best practices in order to inform and develop guidance on how to effectively manage cyber supply chain risks. Proceedings from the workshop as well as referenced case studies and other relevant documents are available at this website.

ITL Withdraws Six Federal Information Processing Standards (FIPS)

A Federal Register Notice on October 19, 2015, announced the withdrawal of the following FIPS:

- FIPS 181, Automated Password Generator (APG);
- FIPS 185, Escrowed Encryption Standard (EES);
- FIPS 188, Standard Security Label for Information Transfer;
- FIPS 190, Guideline for the Use of Advanced Authentication Technology Alternatives;
- FIPS 191, Guideline for the Analysis of Local Area Network Security; and
- FIPS 196, Entity Authentication Using Public Key Cryptography.

ITL withdrew these FIPS because they are obsolete and have not been updated to reference current or revised voluntary industry standards, federal specifications, or federal data standards. Federal agencies are responsible for using current voluntary industry standards and current federal specifications and data standards in their acquisition and management activities. See the FIPS website for more information.

NSTIC Introduces Three New Pilots

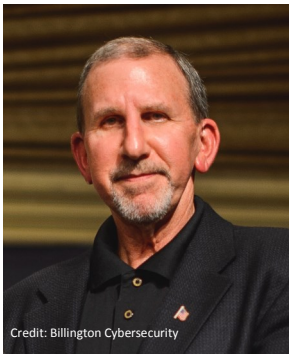
ITL's National Strategy for Trusted Identities in Cyberspace (NSTIC) National Program Office announced the addition of three new pilots to their Pilots Program: MorphoTrust USA, HealthIDx, and Galois, Inc. These pilots are designed to seed the marketplace with NSTIC-aligned identity solutions and address tough identity conundrums associated with everyday transactions. The pilots are aimed specifically at reducing tax refund theft, improving the security of medical information, and providing secure online storage for Internet of Things-enabled devices. This year's selections demonstrate the transition of the pilots program to focus on filling more specific critical gaps in the marketplace. The three new pilots join the ranks of 15 active NSTIC pilots and alumni. The pilots have brought together over 130 partner firms and organizations in support of advancing the NSTIC across 10 major industry sectors. See more about NSTIC pilots at this website.

ITL Participates in Updating Standards for Homeland Security Applications

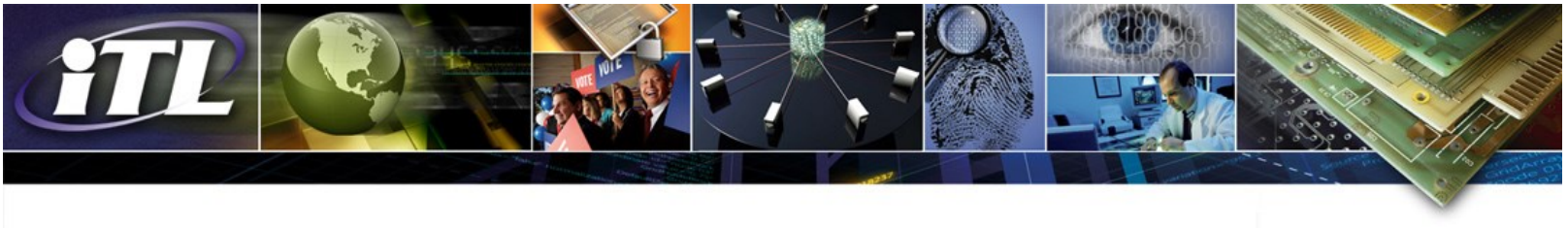
An ITL statistician recently attended a Radiation and Nuclear Detection Standards Working Group meeting at Lawrence Livermore National Laboratory. The working group consisted of representatives from U.S. National Laboratories, the Department of Homeland Security, and NIST who are actively involved in updating national (ANSI and ASTM) and international (IEC) standards for radiation and nuclear detection for homeland security applications. ITL presented recent work done at NIST on the impact that the coefficient of variation in instrument exposure rate readings has on the ability to identify a change in instrument performance when an instrument is subjected to an influence quantity such as an increased temperature or electromagnetic field. The goal of the presentation and subsequent discussion was to illustrate the need for the working group to recognize and consider instrument measurement uncertainty when developing tests and requirements for standards.

Staff Accomplishments

ITL's **Leah Kauffman, Nathan Lesser, Timothy McBride, Gavin O'Brien**, **Lucy Salah**, **Murugiah Souppaya**, **Karen Waltermire**, and NIST colleagues **Keith Bubar** (Acquisitions), **Kevin Kimball** (NIST Chief of Staff), and **Lauren Didiuk** (Office of the General Counsel) received a 2015 Gold Medal from the Department of Commerce for establishing the National Cybersecurity Center of Excellence (NCCoE) to accelerate adoption of cybersecurity standards and best practices. With industry partnerships, the NCCoE builds practical security reference designs that can be rapidly applied to the real challenges that businesses face today. This achievement includes the Department's first Federally Funded Research and Development Center (FFRDC) and the Nation's first FFRDC devoted wholly to cybersecurity.


Credit: Billington Cybersecurity

NIST Fellow **Ronald Ross** received the Samuel J. Heyman Service to America Medal in Homeland Security and Law Enforcement for "instituting a state-of-the-art risk assessment system that has protected federal computer networks from cyberattacks and helped secure information critical to our national and economic security." Ross was one of eight winners chosen for their strong commitment to federal service and significant accomplishments in their fields. **Ross** was also inducted into the National Cyber Security Hall of Fame for developing the NIST Risk Management Framework and leading the development of the first set of unified cyber security standards for the federal government. **Ross** was also named 2015 Government IT Executive of the Year by *Government Computer News*.



Selected New Publications

Computer Security Division 2014 Annual Report
Patrick O'Reilly, Editor; Gregory Witte and Larry Feldman, Co-Editors
NIST Special Publication 800-176
August 2015

Title III of the E-Government Act of 2002, entitled the Federal Information Security Management Act (FISMA) of 2002, requires NIST to prepare an annual public report on activities undertaken in the previous year, and planned for the coming year, to carry out responsibilities under this law. The primary goal of the Computer Security Division (CSD), a component of NIST's Information Technology Laboratory (ITL), is to provide standards and technology that protect information systems against threats to the confidentiality, integrity, and availability of information and services. During Fiscal Year 2014 (FY 2014), CSD successfully responded to numerous challenges and opportunities in fulfilling that mission. Through CSD's diverse research agenda and engagement in many national priority initiatives, high-quality, cost-effective security and privacy mechanisms were developed and applied that improved information security across the federal government and the greater information security community. This annual report highlights the research agenda and activities in which CSD was engaged during FY 2014.

Technical Evaluation, Testing, and Validation of the Usability of Electronic Health Records: Empirically Based Use Cases for Validating Safety-Enhanced Usability and Guidelines for Standardization
By Svetlana Z. Lowry, Mala Ramaiah, Sheryl Taylor, Emily S. Patterson, Sandra Spickard Prettyman, Debora Simmons, David Brick, Paul Latkany, and Michael C. Gibbons
NISTER 7804-1
October 2015

This document provides the empirical rationale for critical patient safety-related usability guidelines for standardization and requirements for validation testing to ensure safety-enhanced design. These standardization guidelines are targeted at eliminating never events and associated patient harm by proactively addressing and mitigating the root causes of use errors from Electronic Health Record (EHR) design and implementation elements, as characterized in our framework on the relationship between usability and patient safety (NISTIR 7804). Requirements for validation testing are instantiated through realistic use cases (that were developed in the course of this research) can be applied during design and evaluation of EHR systems and for user performance testing. The ultimate goal is to drive and empower effective and safe human performance in the use of EHRs.

Security of Interactive and Automated Access Management Using Secure Shell (SSH)
By Tatu Ylonen, Paul Turner, Karen Scarfone, and Murugiah Souppaya
NISTIR 7966
October 2015

Users and hosts must be able to access other hosts in an interactive or automated fashion, often with very high privileges, for a variety of reasons, including file transfers, disaster recovery, privileged access management, software and patch management, and dynamic cloud provisioning. This is often accomplished using the Secure Shell (SSH) protocol. The SSH protocol supports several mechanisms for interactive and automated authentication. Management of this access requires proper provisioning, termination, and monitoring processes. However, the security of SSH key-based access has been largely ignored to date. This publication assists organizations in understanding the basics of SSH interactive and automated access management in an enterprise, focusing on the management of SSH user keys.

Systematic Measurement of Marginal Mark Types on Voting Ballots
By Andrea Bajcsy, Ya-Shian Li-Baboud, and Mary Brady
NISTIR 8069
July 2015

The presence of marginal marks on voting ballots is a known problem in voting systems and has been a source of dispute during federal and state-level elections. As of today, marginal marks are neither clearly countable as votes or as non-votes by optical mark scanners. We aim to establish quantitative measurements of marginal marks in order to provide an objective classification of ballot-mark types and ultimately improve algorithms in optical scanners. By utilizing 800 publicly available manually marked ballot image scans from the 2009 Humboldt County, California, election, we established a set of unique image features that distinguish between votes, non-votes, and five marginal mark types (check mark, cross, partially filled, overfilled, lightly filled). The image features are related to semantic labels through both unsupervised and supervised machine-learning methods. We demonstrate the feasibility of developing an automated and quantifiable set of custom features to improve marginal mark accuracy by 4 to 8 percent, depending on classification model.

Tattoo Recognition Technology – Challenge (Tatt-C): Outcomes and Recommendations
By Mei Ngan, George W. Quinn, and Patrick Grother
NISTIR 8078
September 2015

Tattoos have been used for many years to assist law enforcement in investigations leading to the identification of both criminals and victims. A tattoo is an elective biometric trait that contains additional discriminative information to support person identification and investigation than traditional soft biometrics such as age, gender, and race. While some research has been done in the area of image- based tattoo detection and retrieval, it is not a mature domain. There were no common datasets to evaluate and develop operationally relevant tattoo recognition applications. To address this, NIST conducted the Tattoo Recognition Technology - Challenge (Tatt-C), an initial research challenge that provided operational data and use cases to engage the research community into advancing research and development into automated image-based tattoo technologies and to assess the state of the art to determine what methods are effective and viable for five pertinent operational scenarios.

Upcoming Technical Conferences

NICE Conference and Expo 2015
Dates: November 3-4, 2015
Place: San Diego, California
Cost: Industry $395; Government $225; Academia $199; Student $50; Lunch Ticket $50

The National Initiative for Cybersecurity Education (NICE) 2015 Conference and Expo will feature thought leaders from education, government, industry and nonprofits who are addressing the cybersecurity education, training, and workforce needs of the nation. This two-day event includes face-to-face convening of public-private partners, an opportunity to signal NICE strategic directions and priorities, and a forum to showcase best practices.

NIST contact: William Newhouse

Numerical Reproducibility at Exascale
Date: November 20, 2015
Place: Supercomputing Conference '15, Austin, Texas
Sponsors: NIST, co-located with SC '15

This workshop will address the scope of the problems of numerical reproducibility in high-performance computing in general and those anticipated as we scale to Exascale machines in the next decade. Areas of interest include case studies of reproducibility or the lack of it; reproducibility issues in current HPC; system-level solutions; algorithmic solutions; software solutions; uncertainty quantification in computational reproducibility; fundamental numerical analysis of reproducibility; and future prospects.

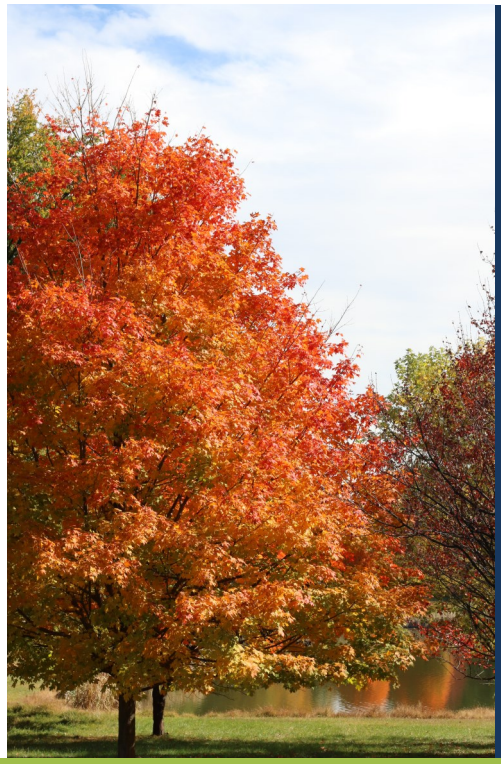
NIST contacts: Walid Keyrouz and Michael Mascagni

Applying Measurement Science in the Identity Ecosystem - NSTIC
Dates: January 12-13, 2016
Place: NIST, Gaithersburg, Maryland
Sponsor: National Strategy for Trusted Identities in Cyberspace (NSTIC)
Cost: TBD

NSTIC's National Program Office will host this technical workshop that will bring together leading security practitioners, experts, and policy makers from across sectors to collaborate about ways to measure and compare the performance of key solutions in the Identity Ecosystem. The goal of the workshop is to improve the measurement science behind identity assurance, so that federal agencies and industry will benefit from better tools to evaluate the performance of solutions.

NIST contact: Paul Grassi

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 at Gaithersburg, MD.

Credit: Katherine Green

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