Information Technology Laboratory Newsletter


Credit: Shutterstock

July—August 2016

Issue 142

INSIDE THIS ISSUE

ITL Leads National Initiative for Cybersecurity Education (NICE)

To meet the growing demand for a trained cybersecurity workforce, ITL leads the National Initiative for Cybersecurity Education (NICE), established by the 2008 Comprehensive National Cybersecurity Initiative (CNCI). Recently, the Cybersecurity Enhancement Act of 2014 called for NICE to develop a strategic plan that was delivered to Congress in April 2016. NICE energizes and promotes a robust network and an ecosystem of cybersecurity education, training, and workforce development. To fulfill this mission, NICE coordinates with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals.

To help meet the NICE goals, NICE supports annual conferences that convene thought leaders from academia, industry, government, and nonprofits. In particular, this year's 7th annual NICE Conference and Expo and the National K-12 Cybersecurity Education Conference will include face-to-face convening of public-private partners, an opportunity to signal NICE strategic directions and priorities, and a forum to showcase innovation and successful initiatives. Additionally, NICE convenes federal government partners for communication and coordination of policy initiatives and strategic directions. The NICE Interagency Coordinating Council provides an opportunity for NICE to communicate program updates and to hear from key partners in the federal government regarding their activities in support of NICE goals and objectives.

Over the past several months, NICE has initiated multiple new efforts to support the mission and goals identified in the Strategic Plan. Efforts include:

- NICE Working Group – provides a mechanism for public and private sector participants to design strategies and pursue actions to advance cybersecurity workforce development;
- NICE eNewsletter – gives regular updates of key NICE programs and projects;
- NICE Webinars – offers ways to enhance the development of the cybersecurity workforce;
- Federal Funding Opportunity - enhances Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development;
- Cybersecurity Jobs Heat Map – As part of the U.S. Department of Commerce's "Skills for Business" initiative, NICE is funding the development of a visualization tool to show the demand for and availability of critical cybersecurity jobs; and
- NICE Challenge Project – a flexible set of challenge environments and supporting infrastructure in which one would be able to perform the tasks outlined in the NICE Workforce Framework.

Colloquium on Quantifying the Weight of Forensic Evidence

ITL and NIST's Special Programs Office recently co-organized the first Technical Colloquium on Quantifying the Weight of Forensic Evidence at NIST Gaithersburg. Approximately 75 attendees took part on site, with another 100 participating via webcast. Intense discussion and exchange of ideas took place among the participants about the theories, methods, and implementation of techniques for quantifying the weight of forensic evidence. These topics are of great relevance to the forensic science, legal, and law enforcement communities. This event was the first in a series of colloquia, with the next event taking place during the summer of 2017. Colloquium proceedings are available.

Vulnerability Test Suite Generator Tool

ITL developed a vulnerability test suite generator tool, VTS, which, since its release in the fall of 2015, has been used by security researchers for testing software assurance tools. The tool produces a collection of test cases to evaluate static source code security analyzers. The test cases are synthetic programs with security weaknesses, as well as corresponding programs without weaknesses (to test for false positives). The weaknesses are embedded within various code constructs representing the kinds of complexities encountered in software. Having a large collection of diverse test cases in different programming languages makes it possible to evaluate different aspects of static analyzers and to improve their performance. The test suite was designed by ITL's Software Assurance Metrics and Tool Evaluation (SAMATE) team members Bertrand Stivalet and Aurelien Delaitre and implemented by students from TELECOM Nancy, France. See the website.

Trustworthy Suppliers Framework

ITL and the Institute for Defense Analyses (IDA) recently co-hosted a forum introducing the Trustworthy Suppliers Framework (TSF). The TSF used NIST Special Publication 800-161, *Supply* Chain Risk Management Practices for Federal Information Systems and Organizations, as a foundation for mapping product and supplier standards, regulations, and policies in the electronic component product category. The goal of the TSF is to allow suppliers flexibility in expressing how they may meet user requirements through demonstrated compliance to various international standards they already use. Similarly, the TSF may allow users to better identify and express their requirements in the procurement process. Attendees worked through two scenarios adapted from NIST SP 800-161 and provided feedback to IDA and NIST on the usefulness and validity of the TSF.

Named Data Networking

ITL recently conducted a workshop on Named Data Networking (NDN) at NIST. The event focused on discussing the role of NDN, one of the most promising future Internet architectures, in support of the Internet of Things and Big Data. With 150 participants, the workshop served as a forum for sharing research results and exchanging ideas among government, industry, and academia as well as an opportunity to build new collaborations. The event featured keynotes by invited speakers, plenary sessions, panels, posters, and demonstrations. Additional information including the archived webcast can be found at the workshop website.

Staff Accomplishments

Computer scientist **Ellen Voorhees** received the Mathematics and Computer Science Award from the Washington Academy of Sciences in recognition of her groundbreaking research and prolific contributions to the fields of computer science and information retrieval. With this award, Voorhees becomes a Fellow of the Washington Academy of Sciences.

Physicist **Stephen Jordan** was selected as a co-winner of the 2016 Katharine Gebbie Young Investigator Award. Sponsored by NIST's chapter of Sigma Xi, this award recognizes exceptional fundamental science in support of the NIST mission by a researcher with less than ten years of professional experience. Jordan was cited for his groundbreaking research in quantum algorithms, which are providing insight into the potential power of future computers which exploit the principles of quantum mechanics.

ITL Director **Charles Romine** received the Arthur S. Flemming Award for his outstanding leadership and management in information technology standards, measurement, and research. The awards are presented by the Arthur S. Flemming Commission and the George Washington University Trachtenberg School of Public Policy and Public Administration, in cooperation with the National Academy of Public Administration. The Flemming Awards honor outstanding federal employees with three to fifteen years of federal service for their exceptional contributions to the federal government.

Selected New Publications

The Twenty-Fourth Text REtrieval Conference Proceedings (TREC 2015)

Ellen Voorhees and Angela Ellis, Editors
NIST Special Publication 500-319
February 2016

This report constitutes the proceedings of the Twenty-Fourth Text REtrieval Conference (TREC 2015) held in Gaithersburg, Maryland, on November 17--20, 2015. The conference was cosponsored by NIST and the Defense Advanced Research Projects Agency (DARPA).

Representation of PIV Chain-of-Trust for Import and Export

By Hildegard Ferraiolo, Ramaswamy Chandramouli, Ketan Mehta, Jason Mohler, Stephen Skordinski, and Steven Brady
NIST Special Publication 800-156
May 2016

This document provides a common XML-based data representation of a chain-of-trust record to facilitate the exchange of PIV Card enrollment data. The exchanged record is the basis to personalize a PIV Card for a transferred employee and also for service providers to personalize a PIV Card on behalf of client federal agencies.

Derived PIV Application and Data Model Test Guidelines

By David Cooper, Hildegard Ferraiolo, Ramaswamy Chandramouli, Nabil Ghadiali, Jason Mohler, and Steven Brady
NIST Special Publication 800-166
June 2016

NIST Special Publication (SP) 800-157 contains technical guidelines for the implementation of standards-based, secure, reliable, interoperable Public Key Infrastructure (PKI)-based identity credentials that are issued for mobile devices by federal departments and agencies to individuals who possess and prove control over a valid Personal Identity Verification (PIV) Card. This document, SP 800-166, contains the requirements and test assertions for testing the Derived PIV Application and associated Derived PIV data objects implemented on removable hardware tokens and within mobile devices. The tests reflect the design goals of interoperability and interface functions.

Measuring the Usability and Security of Permuted Passwords on Mobile Platforms

By Kristen K. Green, John Kelsey, and Joshua M. Franklin
NISTIR 8040
April 2016

This document reports a method of optimizing the input of randomly generated passwords on mobile devices via password permutation to allow for a comparison of password usability data. The number of keystrokes saved - the efficiency gained - via permutation depends on the number of onscreen keyboard changes required in the original password rather than on password length. Additionally, ITL scientists created and are releasing Python scripts (publicly available from https://github.com/usnistgov/PasswordMetrics) for the experiments on entropy loss conducted across passwords ranging in length from 5 to 20 characters.

Report on Post-Quantum Cryptography

By Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone
NISTIR 8105
May 2016

The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks. This report shares NIST's current understanding about the status of quantum computing and post-quantum cryptography, and outlines NIST's initial plan to move forward in this space. The report also recognizes the challenge of moving to new cryptographic infrastructures and therefore emphasizes the need for agencies to focus on crypto agility.

Applied and Computational Mathematics Division: Summary of Activities for Fiscal Year 2015

Ronald Boisvert, Editor
NISTIR 8132
May 2016

This report summarizes recent technical work of ITL's Applied and Computational Sciences Division from October 2014 to December 2015. Following a high-level overview of the Division's activities, the report provides further details on eight projects of particular note during the reporting period. The next section gives brief synopses of all technical projects active during the past year. Finally, the report lists publications, technical talks, and other professional activities in which division staff members participated.

Identifying and Categorizing Data Types for Public Safety Mobile Applications Workshop Report

By Michael Ogata
NISTIR 8135
May 2016

The Association of Public-Safety Communications (APCO), in cooperation with FirstNet and the Department of Commerce, held a workshop on June 2, 2015, entitled "Identifying and Categorizing Data Types for Public Safety Mobile Applications." The goal of the workshop was to identify different types of data that will flow through applications that operate on the National Public Safety Broadband Network (NPSBN). A diverse group of first responders, industry leaders, and government representatives attended the workshop. This document describes the workshop and captures the input received from attendees.

Upcoming Technical Conferences

NIST Workshop on Software Measures and Metrics to Reduce Security Vulnerabilities
Date: July 12, 2016
Place: NIST, Gaithersburg, Maryland
Cost: None

With useful metrics, it is straightforward to determine which software development technologies or methodologies lead to sustainably secure systems. The goal of this workshop is to gather ideas on how the federal government can best use taxpayer money to identify, improve, package, deliver, or boost the use of software measures and metrics to significantly reduce security vulnerabilities.

NIST contacts: Elizabeth Fong, elizabeth.fong@nist.gov
Paul Black, paul.black@nist.gov

NSCI Seminar: Accelerating Discovery Via Science Services
Date: August 2, 2016
Place: NIST, Gaithersburg, Maryland
Cost: None
Sponsor: National Strategic Computing Initiative (NSCI) Committee

To address the issue of exploding volumes of data, Ian Foster, University of Chicago and Argonne National Laboratory, will explore the past, current, and potential future of large-scale outsourcing and automation for science, and suggest opportunities and challenges for today's researchers.

NIST contact: Barry Schneider, barry.schneider@nist.gov

Global Identity Summit
Dates: September 19-21, 2016
Place: Tampa, Florida
Cost: $395—$795

Organized by the Armed Forces Communications and Electronics Association, the Global Identity Summit is the U.S. federal government's primary outreach and collaboration-building event with the worldwide identity community each year.

NIST contacts: Michael Garris, michael.garris@nist.gov
Paul Grassi, paul.grassi@nist.gov

NSCI Seminar: Leading-Edge Computers and the Extraordinary Research They Enable
Date: October 4, 2016
Place: NIST, Gaithersburg, Maryland
Cost: None
Sponsor: National Strategic Computing Initiative (NSCI) Committee

Thomas H. Dunning Jr., Pacific Northwest National Laboratory and the University of Washington, will describe a new generation of supercomputers, illustrate the role that they play or will play in a few areas of research, and describe the challenges facing the development of exascale modeling and simulation.

NIST contact: Barry Schneider, barry.schneider@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 at Gaithersburg, MD.

Credit: Katherine Green

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