Information Technology Laboratory Newsletter

Credit: Shutterstock

March—April 2016

Issue 140

INSIDE THIS ISSUE

ITL FOCUSES ON COMMON DATA FORMAT FOR ELECTION RESULTS

For the 2016 Presidential Election, the State of Ohio will implement changes to its election management systems using the recently published NIST Special Publication (SP) 1500-100, *A Common Data Format for Election Results Reporting.* SP 1500-100 specifies a common data format for pre-election and post-election data from election management systems (EMS) used for managing elections and tabulating election results across states and territories of the United States. Several other states are currently investigating and updating their election systems to use the specification.

This specification was developed to reduce the complexity for U.S. election officials in collecting and publishing election data to news outlets and the public, especially on election night when time frames are tight and there are more opportunities for error. The process of reporting election results is a highly complicated activity. The EMS generally do not interoperate, adding more complexity to the process. Additionally, there are significant variations in election results reporting among different jurisdictions.

NIST and a community of U.S. election officials, analysts, and voting system manufacturers investigated reporting scenarios and their associated geopolitical geographies throughout the United States. They looked at existing and emerging voting systems. From this analysis, the specification was developed to allow election offices to report on data known ahead of the election such as detailed ballot information, on election night data, and then during the post-election phase as updates and final results are compiled. The specification includes the capability to handle very detailed data that includes the basic results from contests, as well as analysis of the different types of ballots used, the actual voting systems used at polling places, and errors typically made on ballots by voters that result in overvotes and undervotes.

For more information, visit ITL's voting website.

ITL's National Cybersecurity Center of Excellence (NCCoE) Expands Facilities to Accommodate Growth

The NCCoE recently moved from its office at the Universities of Shady Grove into a fully renovated building at 9700 Great Seneca Highway in Rockville, Maryland, to accommodate continued program growth. The new NCCoE office is approximately six times larger than the old space, with 22 labs and space to host events.

Federal officials and lawmakers gather for the opening of the new National Cybersecurity Center of Excellence Feb. 8.(Photo: NIST)

To celebrate the new building, NIST and the NCCoE hosted a Dedication Ceremony on February 8, 2016. Secretary of Commerce Penny Pritzker and Maryland Senator Barbara Ann Mikulski participated in the ribbon cutting and provided remarks. The event also featured building tours and presentations of current projects. See the NCCoE website.

NIST Cloud Computing Definition Highly Cited and Used as Resource for Coursework

In early 2007, ITL computer scientists undertook research to define cloud computing, describe the salient security issues, and recommend steps to safely use the extraordinary potential of cloud computing. Specifically, ITL produced a series of publications: NIST Special Publication (SP) 800-144, *Security and Privacy of Public Cloud Computing;* NIST SP 800-145, *NIST Definition of Cloud Computing; and* NIST SP 800-146*, Cloud Computing Synopsis and Recommendations,* all available at ITL's Cloud Computing website.

To date, the NIST definition of cloud computing has been cited more than 6,000 times, according to Google Scholar. Moreover, the NIST publications form the basis of coursework developed by IEEE. Subsequently, IEEE and EdX developed Massive Online Open Course material that incorporated the NIST source material. To date, more than 100,000 people from 179 countries have sampled these courses. More information on these courses is available at the IEEE Education & Careers website.

ITL Conducts Workshop on Measurement Science in the Identity Ecosystem

ITL recently conducted a technical workshop on "Applying Measurement Science in the Identity Ecosystem." The 220 participants included leading security practitioners, solution providers, experts, and policy makers from across sectors. The purpose of the workshop was to improve the science behind identity assurance so federal agencies and industry will have better tools to measure the performance of solutions. During informative expert panels and intensive breakout sessions, attendees brainstormed and evaluated approaches, barriers, implementation considerations, and market solutions for measurement science in the Identity Ecosystem. The results from this workshop will guide the next steps in creating effective identity proofing processes and metrics for federal agencies and industry. See the National Strategy for Trusted Identities in Cyberspace website.

Staff Accomplishments

Ronald Ross, NIST Fellow in ITL's Computer Security Division, was selected by GovInfoSecurity for its seventh annual list of top influencers - lawmakers, top government officials, practitioners, and thought-leaders whose leadership has a substantial influence on government cybersecurity policy. Ross was recognized as one of the world's leading risk management authorities. In addition, Ross received a Federal 100 Award from *Federal Computer Week* for his contributions to the security of federal information systems.

Adam Sedgewick, Senior Advisor in the Office of the ITL Director, was named by GovInfoSecurity as one of the top influencers of 2016 on government cybersecurity policy. Sedgewick was selected for his contributions to the NIST Cybersecurity Framework. Influencers demonstrated outstanding leadership and collaborative abilities.

Donna Dodson, Chief Cybersecurity Adviser and Director of ITL's National Cybersecurity Center of Excellence, was named by MeriTalk as one of the top women in government IT. Dodson was recognized for her management of ITL's cybersecurity research program and her ability to develop relationships with academia, industry, and government agencies to brainstorm

Selected New Publications

Mobile ID Device Best Practice Recommendation Version 2.0
By Bradford Wing
NIST Special Publication 500-280v2
November 2015

Version 1 of the Mobile ID Best Practice Recommendation (BPR) has been referenced in many government procurement acquisitions and has provided information helpful to companies developing mobile ID solutions. This version of the BPR builds upon that solid foundation, reflecting changes in technology, the operating environment, and standards. Although closely tied to the ANSI/NIST-ITL standard in content, this is a separate document and may be used independently of the standard.

Framework for Cloud Usability
By Brian Stanton, Mary Theofanos, and Karun P. Joshi
NIST Special Publication 500-316
December 2015

Organizations are increasingly adopting cloud-based services to meet their business needs. However, due to the complexity and diversity of cloud systems, it is important to evaluate the user experience within a framework that encompasses the characteristics that define the user experience. In this paper, we propose a cloud usability framework to provide a structure to evaluate the key attributes of the cloud user experience. The framework includes five attributes and twenty elements that characterize the user experience. The framework can be the foundation for developing usability metrics for organizations interested in measuring the user experience when adopting the cloud.

Recommendation for Key Management Part 1: General (Revision 4)
By Elaine B. Barker
NIST Special Publication 800-57 Part 1
January 2016

This Recommendation provides cryptographic key management guidance. It consists of three parts. Part 1 provides general guidance and best practices for the management of cryptographic keying material. Part 2 provides guidance on policy and security planning requirements for U.S. government agencies. Finally, Part 3 provides guidance when using the cryptographic features of current systems.

Simple Guide for Evaluating and Expressing the Uncertainty of NIST Measurement Results
By Antonio Possolo
NIST Technical Note 1900
October 2015

This document serves as a succinct guide to evaluating and expressing the uncertainty of NIST measurement results, for NIST scientists, engineers, and technicians who make measurements and use measurement results, and also for our external partners—customers, collaborators, and stakeholders. It supplements but does not replace NIST Technical Note 1297, whose guidance and techniques may continue to be used when they are fit for purpose and there is no compelling reason to question their applicability.

The Influence of Realism on Congestion in Network Simulations
By Kevin Mills and Christopher Dabrowski
NIST Technical Note 1905
January 2016

This paper examines the influence of realism on the spread of congestion in network simulations. We begin with an abstract network simulation, taken from the literature, and add elements of realism in various combinations, culminating with a high-fidelity simulation, also taken from the literature. By comparing patterns of congestion among combinations, we make four main contributions. We hope our contributions lead to better understanding of the influence of realism on congestion in network simulations, and to improved dialog throughout the diverse community of researchers who rely on network simulations.

Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (Vol. 1), and *Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity* (Vol. 2)
Michael Hogan and Elaine Newton, Editors
NISTIR 8074, Vols. 1 and 2
December 2015

This report sets out proposed U.S. government strategic objectives for pursuing the development and use of international standards for cybersecurity and makes recommendations to achieve those objectives. The recommendations cover interagency coordination, collaboration with the U.S. private sector and international partners, agency participation in international standards development, standards training and education, use of international standards to achieve mission and policy objectives, and other issues.

Critical Workflow and Exception Handling in EHR Design for Highly Infectious Diseases
By Svetlana Lowry, Mala Ramaiah, E.S. Patterson, L.A. Paul, D. Simmons, D. Brick, and M.C. Gibbons
NISTIR 8095
December 2015

Adoption of Electronic Health Records (EHRs) in all care settings has become widespread. EHRs can support and revolutionize the way that public health is protected in the event of an outbreak of a highly infectious disease. In this report, infectious disease experts provide insights about patient safety and workflow considerations that arose during their experiences treating patients suspected of having Ebola. These insights provide a first step in creating an effective infrastructure to better identify, diagnose, treat, and report infectious diseases in the United States.

Upcoming Technical Conferences

29th Annual Federal Information Systems Security Educators' Association (FISSEA) Conference
Dates: March 15-16, 2016
Place: NIST, Gaithersburg, Maryland
Sponsors: NIST and FISSEA
Cost: $140 with Catering

The annual FISSEA conference serves as a forum for the exchange of information about information security awareness, training, education, and certification. The theme of this year's conference is "The Quest for the Un-Hackable Human: The Power of Cybersecurity Awareness and Training."

NIST contact: Peggy Himes, peggy.himes@nist.gov

Hands-On Workshop on Assessing and Reporting Measurement Uncertainty
Dates: March 23-25, 2016
Place: Anaheim, California
Cost: $1,095

This short course covers the propagation of measurement uncertainty using the methods outlined in the Joint Committee for Guides in Metrology Guide to the Expression of Uncertainty in Measurement from a statistical perspective. The course will provide participants with a working knowledge of the computational methods needed to assess measurement uncertainty, hands-on experience in the application of these methods, and scientific and statistical insight into the interpretation of the results.

Conference website: http://www.msc-conf.com/
NIST contacts: Will Guthrie, william.guthrie@nist.gov
Hung-Kung Liu, hung-kung.liu@nist.gov

Cybersecurity Framework Workshop 2016
Dates: April 6-7, 2016
Place: NIST, Gaithersburg, Maryland
Cost: None

In addition to highlighting a variety of Framework use, the purpose of this workshop is to gather input to help NIST understand stakeholder awareness and current use of the Framework, the need for an update to the Framework, cybersecurity best practices sharing, and the future governance of the Framework.

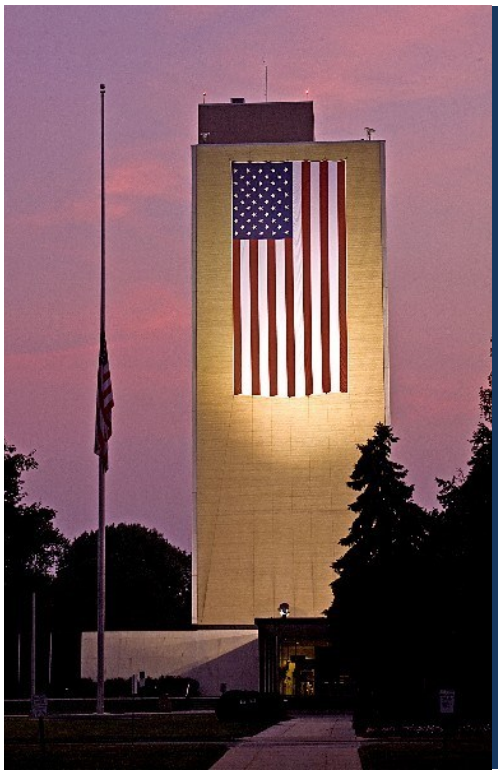
NIST contact: Matthew Barrett, matthew.barrett@nist.gov

Random Bit Generation Workshop 2016
Dates: May 2-3, 2016
Place: NIST, Gaithersburg, Maryland
Cost: None

NIST is in the process of completing the development of approved methods for random bit generation.
SP 800-90A has recently been revised. SP 800-90B addresses the entropy sources needed to seed the DRBG mechanisms. A new draft of SP 800-90B is available for public comment. SP 800-90C specifies constructions for creating random bit generators from entropy sources and DRBG mechanisms. A new draft of this document will be available for review and comment prior to the workshop. The workshop will discuss SP 800-90B and SP 800-90C, as well as their validation by NIST's validation programs.

NIST contacts: RBG Workshop Team, rbg_workshop@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

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

The NIST campus at Gaithersburg, MD.

Credit: NIST