Information Technology Laboratory Newsletter

INSIDE THIS ISSUE

January—February 2016

Issue 139

Credit: Jim Ashby, retired Western Regional Climate Center

Automated surface observing station in Milford, Utah.

ITL FOCUSES ON EXTREME WIND SPEEDS

When a unique research opportunity comes along, ITL researchers welcome the challenges. ITL statisticians are often called upon to collaborate with researchers in other NIST laboratories. Such was the case in a recent study of extreme wind speeds, carried out jointly between ITL's Statistical Engineering Division and NIST's Materials and Structural Systems Division. Researchers collected time histories, some more than 50 years long, of wind gusts for over 1000 meteorological stations. The data from these stations were rigorously checked for quality, and corrections were applied to make the observations comparable between stations. An example of one such correction is the height at which observations are made. The station in Milford, Utah, is typical of automated surface observing stations throughout the United States.

NIST conducted the study to contribute to the American Society of Civil Engineers (ASCE)-7 series of standards, which describe load requirements, e.g., earthquakes, floods, and wind gusts, for common structures. A major part of the standard relating to wind is a set of maps showing estimates of wind speeds with mean recurrence intervals (MRIs) of interest. One such is the 50-year MRI, which can be thought of in this way: If *x* is the wind speed with a 50-year MRI, one gust, achieving speed *x* or greater, is expected in the next 50 years.

Researchers used the collection of time histories to create a set of these maps for non-tornadic, non-hurricane winds in the contiguous United States. To create the initial maps, the time history for each station was modeled, and the model was used to estimate wind speeds for all MRIs of interest. The individual estimates were then smoothed to create maps. NIST Special Publication 500-301, *Maps of Non-hurricane Non-tornadic Wind Speeds with Specified Mean Recurrence Intervals for the Contiguous United States Using a Two-Dimensional Poisson Process Extreme Value Model and Local Regression*, gives a detailed description of how the maps were created.

An important improvement over the maps in the current standard, ASCE7-10, is the recognition of differences in the wind climate between regions. For example, the wind climate in the Midwest is different than the wind climate on the East Coast. The new maps should lead to designs that are consistent with the risk in a given area, allowing for both safety and economy.

ITL's TREC 2015 Project Included Real-Time Tasks

The Text REtrieval Conference (TREC) project creates the infrastructure necessary to measure the quality of search engines. TREC 2015 took place on November 17-20, 2015, at NIST. Eighty-seven teams from 20 countries participated. Each TREC is organized around a set of focus areas called tracks. TREC 2015 included eight tracks that investigated topics ranging from finding clinically relevant information in the biomedical literature given a case narrative, to developing systems that can infer the searcher's real-world task from the submitted query string. Four of the eight tracks were new for 2015.

The problem evaluated in a track is generally an abstraction of one or more real-world search tasks. Abstraction makes tasks easier to evaluate and can make results more generalizable, but care must be taken in defining the abstract task so that results are valid for the real-world tasks. Several 2015 tracks increased the realism of their evaluation task by requiring systems to process data in (near) real time. See the TREC website for more information.

Cryptographic Key Management Guidance for Federal Agencies

ITL recently published two significant documents on cryptographic key management for federal agencies. *NIST Special Publication (SP) 800-152*, A Profile for U. S. Federal Cryptographic Key Management Systems, contains requirements for the design, implementation, procurement, installation, configuration, management, operation, and use of a Key Management System by federal agencies. The second document, *NIST SP 800-131A, Rev. 1*, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, provides guidance for transitioning to the use of stronger cryptographic keys and more robust algorithms by federal agencies when protecting sensitive, but unclassified information.

State of Connecticut Implements NIST Validation Tool for Health Information Technology

The Connecticut Department of Public Health has implemented their Electronic Laboratory Reporting (ELR) system using the NIST Health Level (HL) 7 v2.5.1 ELR Validation Tool. An ITL team develops HL7 v2 conformance tools for health information technology certification testing by the Office of the National Coordinator for Health Information Technology (ONC) related to the Centers for Medicare and Medicaid Services (CMS) Meaningful Use Program. The program awards incentive payments to eligible providers and provider organizations that use ONC-certified products in healthcare delivery in accordance with specified CMS requirements, including public health-related reporting requirements such as submission of data for ELR. The ITL team worked with the Connecticut Department of Public Health to modify the current NIST context-free ELR validation tool to reflect Connecticut-specific ELR requirements. This customized version of the tool is being used by healthcare providers in Connecticut in their on-boarding process in preparation for submission of reportable laboratory test results.

Staff Accomplishments

Kamran Sayrafian received the Department of Commerce Bronze Medal for his leadership in establishing an internationally recognized NIST research program in body-area networking (BAN).

Jonathan Fiscus, David Joy, Gregory Sanders, Martial Michel, Paul Over, Darrin Dimmick, John Garofolo, and **Angela Ellis** received the Department of Commerce Bronze Medal for significant technical contributions providing the measurement science infrastructure needed to advance the state of the art in automated video/ multimedia analysis.

The ITL quantum research team **Xiao Tang, Oliver Slattery, Paulina Kuo,** and **Barry Hershman** received the Department of Commerce Bronze Medal for the development of quantum frequency conversion systems that convert single photons in the telecommunications frequency bands to the visible region with near 100 percent internal efficiency.

Emanuel Knill received the NIST Samuel Wesley Stratton Award for his pioneering work in the field of quantum information science and engineering. He developed a mathematical foundation for exploiting the rules of quantum mechanics to create novel computing devices with a phenomenal increase in storage and processing capability.

Selected New Publications

National Checklist Program for IT Products - Guidelines for Checklist Users and Developers

By Stephen D. Quinn, Murugiah Souppaya, Melanie Cook, and Karen Scarfone
NIST Special Publication 800-70 Rev 3
December 2015

A security configuration checklist is a document that contains instructions or procedures for configuring an information technology (IT) product to an operational environment, for verifying that the product has been configured properly, and/or for identifying unauthorized changes to the product. Using these checklists can minimize the attack surface, reduce vulnerabilities, lessen the impact of successful attacks, and identify changes that might otherwise go undetected. To facilitate development of checklists and to make checklists more organized and usable, ITL established the National Checklist Program (NCP), where users can find and retrieve checklists. The document describes the policies, procedures, and general requirements for participation in the NCP.

NIST Big Data Interoperability Framework

NIST Big Data Public Working Group; Wo Chang, Editor
NIST Special Publication 1500, Vols. 1-7
October 2015

Big Data is a term used to describe the large amount of data in the networked, digitized, sensor-laden, information-driven world. While opportunities exist with Big Data, the data can overwhelm traditional technical approaches and the growth of data is outpacing scientific and technological advances in data analytics. To advance progress in Big Data, the NIST Big Data Public Working Group (NBD-PWG) is working to develop consensus on important fundamental concepts related to Big Data. The results are reported in the NIST Big Data Interoperability Framework series of volumes.

Volume 1, Definitions; Volume 2, Big Data Taxonomies; Volume 3**,** Use Cases and General Requirements;
Volume 4, Security and Privacy; Volume 5, Architectures White Paper Survey; Volume 6, Reference Architecture; and Volume 7, Standards Roadmap.

Trusted Geolocation in the Cloud: Proof of Concept Implementation

By Michael Bartock, Murugiah Souppaya, Raghuram Yeluri, Uttam Shetty, James Greene, Steve Orrin, Hemma Prafullchandra, John McLeese, Jason Mills, Daniel Carayiannis, Tarik Williams, and Karen Scarfone
NISTIR 7904
December 2015

This publication explains selected security challenges involving Infrastructure as a Service (IaaS) cloud computing technologies and geolocation. It describes a proof of concept implementation that was designed to address those challenges. The publication is intended to be a blueprint or template that can be used by the general security community to validate and implement the described proof of concept implementation.

Policy Machine: Features, Architecture, and Specification

By David F. Ferraiolo, Serban Gavrila, and Wayne Jansen
NISTIR 7987 Rev 1
October 2015

The ability to control access to sensitive data in accordance with policy is perhaps the most fundamental security requirement. Despite over four decades of security research, the limited ability for existing access control mechanisms to enforce a comprehensive range of policy persists. This report describes an access control framework, referred to as the Policy Machine (PM), which fundamentally changes the way policy is expressed and enforced. The report gives an overview of the PM and the range of policies that can be specified and enacted.

Cloud-Based Accessibility for Voting Applications By Shanee Dawkins and Sharon Laskowski

NISTIR 8047
November 2015

Since its creation, the National Institute on Disability and Rehabilitation Research (NIDRR) of the U.S. Department of Education has supported the development of new technologies for enhancing access for people with disabilities. Current research and development being conducted by the international Global Public Inclusive Infrastructure Consortium (GPII), drawing on work supported by NIDRR, is creating technology for cloud-based accessibility. Using this new technology, users of computer systems can create personal profiles that specify how computer applications should be configured to meet their individual accessibility needs. ITL researchers evaluated the applicability of this new technology for voting applications. They developed a prototype voting support system with enhanced accessibility capabilities, based on the cloud-based accessibility work of the GPII. This prototype, the Next Generation Voting Platform (NGVP), is a mobile ballot-marking application designed so that voters have the capability to mark a blank ballot via a customized interface.

De-Identification of Personal Information

By Simson L. Garfinkel
NISTIR 8053
October 2015

De-identification removes identifying information from a dataset so that individual data cannot be linked with specific individuals. De-identification can reduce the privacy risk associated with collecting, processing, archiving, distributing or publishing information. In recent years, researchers have shown that some de-identified data can sometimes be re-identified. Many different kinds of information can be de-identified, including structured information, free format text, multimedia, and medical imagery. This document summarizes roughly two decades of de-identification research, discusses current practices, and presents opportunities for future research.

Upcoming Technical Conferences

Applying Measurement Science in the Identity Ecosystem

Dates: January 12-13, 2016
Place: NIST, Gaithersburg, Maryland
Sponsor: NIST
Cost: With Catering: $44; Without Catering: Free

This technical workshop 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, paul.grassi@nist.gov

29th Annual Federal Information Systems Security Educators' Association (FISSEA) Conference

Dates: March 15-16, 2016
Place: NIST, Gaithersburg, Maryland
Sponsors: NIST and FISSEA
Cost: TBD

FISSEA 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

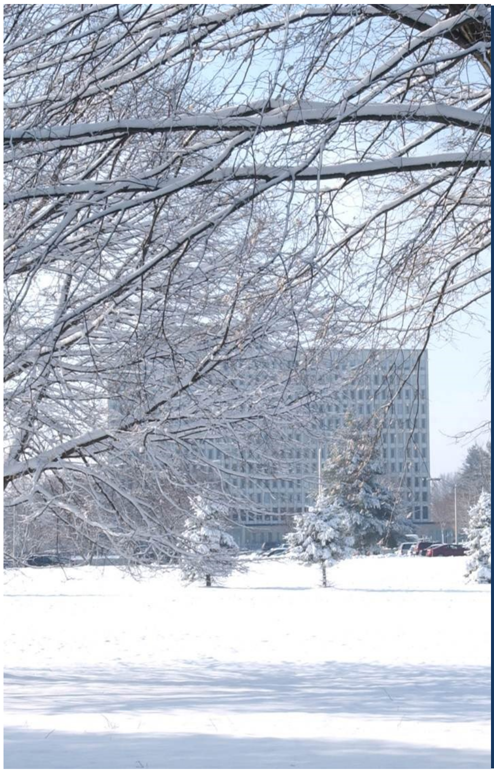
Hands-On Workshop on Assessing and Reporting Measurement Uncertainty

Dates: March 23-25, 2016
Place: Anaheim, California
Cost: TBD

This short course covers the propagation of measurement uncertainty using the methods outlined in the JCGM 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.

NIST contacts: Will Guthrie, william.guthrie@nist.gov
Hung-Kung Liu, hung-kung.liu@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