Information Technology Laboratory Newsletter

Credit: Shutterstock

September—October 2016

Issue 143

INSIDE THIS ISSUE

ITL Focuses on Metrics to Reduce Security Vulnerabilities in Software

The Federal Cybersecurity Research and Development Strategic Plan seeks to fundamentally alter the dynamics of security. The plan calls for "the design and implementation of software, firmware, and hardware that are highly resistant to malicious cyber activities ..." and to reduce the number of vulnerabilities in software by orders of magnitude. Measures of software play an important role.

To identify ways to achieve more secure software, ITL recently held a workshop on “Software Measures and Metrics to Reduce Security Vulnerabilities.” More than 90 people from the federal government, software assurance tool makers, service providers, and universities attended. The object of the workshop was to gather ideas on how the federal government can best identify, improve, package, deliver, or boost the use of software measures and metrics to significantly reduce vulnerabilities.

Twenty position statements were submitted in advance. The workshop program included nine presentations based on accepted position statements as well as one breakout session. The presentations came from the White House Office of Science and Technology Policy, Vector Software, U.S. Naval Research Laboratory, University of Wisconsin-Madison, Software Engineering Institute, NIST, Consortium for IT Software Quality, and BlackBerry.

For the breakout session, attendees were randomly assigned to one of six breakout groups to develop the best ideas to dramatically reduce software vulnerabilities in three to five years. Recommendations included the following:

- Code should be amenable to automatic analysis;
- There should be standard tool outputs;
- Contract and procurement should specify secure and high-quality code;
- Findings about the quality and utility of tools and libraries should be shared;
- Software developers should be liable for egregiously poor software; and
- Programmers should be better educated to understand the need for security.

ITL’s report on the workshop will be available in the fall. Ideas from the workshop will be forwarded to the White House Office of Science and Technology Policy for inclusion in future reports. See our website.

Commission on Enhancing National Cybersecurity

The Commission on Enhancing National Cybersecurity held its 5th public meeting at the University of Minnesota on August 23, 2016. Established in Executive Order 13718, the commission develops detailed short-term and long-term recommendations to strengthen cybersecurity in both the public and private sectors. The Executive Order directs NIST to provide the commission with expertise, services, funds, facilities, staff, equipment, and other support services needed to carry out its mission.

Meeting monthly since the inaugural meeting in April 2016 at the Department of Commerce, the commissioners have established the scope of their task and developed a work plan for meeting the requirements expressed in the Executive Order. See the cybersecurity commission website.

ITL Hosts Gifted Undergraduate Mathematics Students

ITL's Applied and Computational Mathematics Division recently hosted a visit of undergraduate student participants in Morgan State University's Math Summer Program in Research and Learning (SPIRAL) program. The program targets gifted sophomore and juniors from underrepresented groups; this year's participants included students from Spelman College, Morehouse College, Denison University, Clark Atlanta, and American University.

The 12 students and their faculty and graduate student advisors were briefed on the role of mathematics at NIST, and enjoyed presentations and lab visits on graph theory and probability in measurement, scientific visualization, and uncertainty quantification in materials modeling and in force and climate measurement.

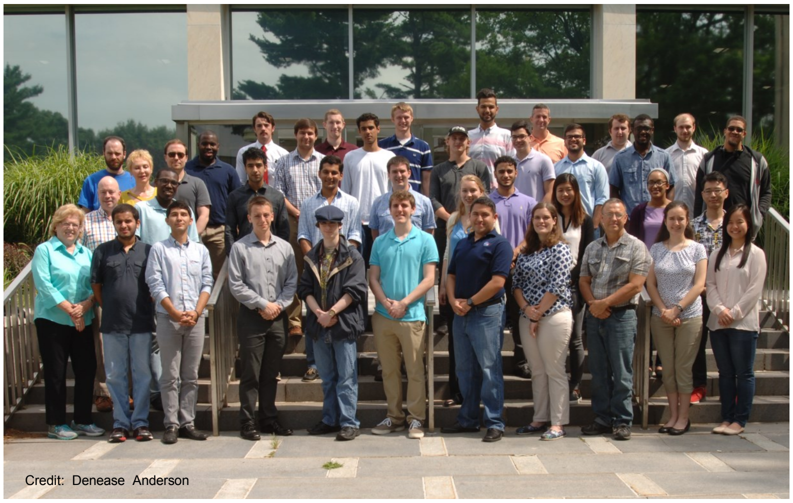
ITL Staffer Co-Chairs Subcommittee on Machine Learning and Artificial Intelligence

Michael Garris, Information Access Division, serves as the Department of Commerce co-chair of the Administration's National Science and Technology Council Subcommittee on Machine Learning and Artificial Intelligence (AI). This group monitors state-of-the-art advances and technology milestones in machine learning and artificial intelligence within the federal government, in the private sector, and internationally, and helps to coordinate federal activity in this space. The subcommittee is tasked with releasing a public roadmap on "AI for the Good" along with a National R&D Strategy, targeted for release in October 2016.

Staff Accomplishments

Ram Sriram, Chief of ITL's Software and Systems Division, received the 2016 Computers and Information Engineering (CIE) Lifetime Achievement Award from the American Society of Mechanical Engineers. Sriram received the award for his leadership in developing innovative computational tools and techniques for automating and integrating the entire engineering enterprise and for developing the next generation of leaders in engineering.

Rodney Petersen, Director of ITL's National Initiative for Cybersecurity Education (NICE), received a 2016 Government Leadership of the Year Award from the Colloquium for Information Systems Security Education (CISSE). CISSE supports cybersecurity educators, researchers, and practitioners in their efforts to improve curricula and foster discussion of current and emerging trends.



Credit: Denease Anderson

This summer ITL and NIST's Communications Technology Laboratory hosted 39 students from 25 colleges and universities in the Summer Undergraduate Research Fellowship (SURF) program, which provides hands-on research experience in applied mathematics, statistics, software testing, computer security, information access, and networking.

Selected New Publications

[Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security](#)
By Murugiah Souppaya and Karen Scarfone
NIST Special Publication 800-46 Rev 2
July 2016

For many organizations, their employees, contractors, business partners, vendors, and/or others use enterprise telework or remote access technologies to perform work from external locations. All components of these technologies, including organization-issued and bring your own device (BYOD) client devices, should be secured against expected threats as identified through threat models. This publication provides information on security considerations for several types of remote access solutions, and it makes recommendations for securing a variety of telework, remote access, and BYOD technologies. It also gives advice on creating related security policies.

Computer Security Division 2015 Annual Report
Patrick D. O'Reilly, Greg Witte, and Larry Feldman, Editors
NIST Special Publication 800-182
July 2016

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. ITL's Computer Security Division (CSD) provides standards and technology that protects information systems against threats to the confidentiality, integrity, and availability of information and services. 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 in FY 2015.

Network of Things
By Jeffrey Voas
NIST Special Publication 800-183
July 2016

System primitives allow formalisms, reasoning, simulations, and reliability and security risk trade-offs to be formulated and argued. In this work, five core primitives belonging to most distributed systems are presented. These primitives apply well to systems with large amounts of data, scalability concerns, heterogeneity concerns, temporal concerns, and elements of unknown pedigree with possible nefarious intent. These primitives are the basic building blocks for a Network of 'Things' (NoT), including the Internet of Things (IoT). This document offers an underlying and foundational science to IoT based on the realization that IoT involves sensing, computing, communication, and actuation. The material presented here is generic to all distributed systems that employ IoT technologies (i.e., 'things' and networks).

Usability and Security Considerations for Public Safety Mobile Authentication
By Yee-Yin Choong, Joshua M. Franklin, and Kristen K. Greene
NISTIR 8080
July 2016

There is a need for cybersecurity capabilities and features to protect the Nationwide Public Safety Broadband Network (NPSBN). Understanding how public safety users operate in their different environments will allow for usable cybersecurity capabilities and features to be deployed and used. Although first responders work in a variety of disciplines, this report is focused on the Fire Service, Emergency Medical Services (EMS), and Law Enforcement. This report describes the constraints presented by the personal protective equipment, specialized gear, and unique operating environments and how such constraints may interact with mobile authentication requirements. The overarching goal of this work is analyzing which authentication solutions are the most appropriate and usable for first responders using mobile devices in operational scenarios.

UPCOMING TECHNICAL CONFERENCES

Privacy Controls Workshop: Next Steps for NIST Special Publication 800-53, Appendix J
Date: September 8, 2016
Place: U.S. Department of Transportation (DOT), Washington, D.C.
Sponsors: NIST and DOT
Cost: None

The purpose of this workshop is to gather input on the privacy options of Appendix J of NIST Special Publication 800-53, Revision 4. The workshop will explore the effectiveness and challenges of applying the current privacy controls in 800-53 and whether changes should be made in the publication's fifth revision. System designers and privacy engineers, privacy officers, senior agency officials for privacy and privacy subject matter experts should attend this interactive workshop.

NIST contact: Suzanne Lightman,
suzanne.lightman@nist.gov

Upcoming Technical Conferences

NIST Cloud Computing Forum & Workshop IX
Dates: September 13-15, 2016
Place: NIST, Gaithersburg, Maryland
Cost: None

Cloud computing allows us to create, store, and manipulate ever-increasing amounts of data from an array of devices which are connected and interact with their environment. The theme of this year's workshop is "Cloud & the Interconnected World." Speakers will address the role of cloud computing in meeting the challenges of an interconnected world and the necessary building blocks for the vision and standards that make an interconnected world possible.

NIST contact: Robert Bohn, robert.bohn@nist.gov

NSCI: High-Performance Computing Security Workshop
Dates: September 29-30, 2016
Place: NIST, Gaithersburg, Maryland
Cost: $99.00
The goal of the President's National Strategic Computing Initiative (NSCI) is to maximize the benefits of High-Performance Computing (HPC) for economic competitiveness and scientific discovery. Security for HPC systems is essential for the systems to provide the anticipated benefits. This workshop will identify security priorities and principles that should be incorporated into the strategy of the NSCI, to bring together stakeholders from industry, academia, and government, and to identify gaps that should be addressed.

NIST contact: Lee Badger, mark.badger@nist.gov

Lightweight Cryptography Workshop 2016
Dates: October 17-18, 2016
Place: NIST, Gaithersburg, Maryland
Cost: $41 with catering; $20 no catering

ITL is assessing the need for a dedicated lightweight cryptography standard. Following an initial workshop in 2015 to solicit public feedback on the requirements and characteristics of real-world applications of lightweight cryptography, ITL is creating a portfolio of dedicated lightweight algorithms through an open process similar to the selection of modes of operation of block ciphers. Algorithm recommendations will be associated with 'profiles' that target a class of devices and applications. This second workshop will focus on issues related to the potential future standardization process of lightweight primitives.

NIST contact: Meltem Turan, meltem.turan@nist.gov

IEEE/NIST Workshop on Timing Challenges in the Smart Grid
Date: October 26, 2016
Place: NIST, Gaithersburg, Maryland
Sponsors: NIST and IEEE Standards Association
Cost: None

The purpose of this workshop is to identify and analyze the practical challenges that are currently being experienced in wide-area time synchronization in current measurement and control deployments as well as timing-related barriers that prevent the power industry from realizing future measurement and control technologies.

NIST contact: Ya-Shian Li-Baboud, ya-shian.li-baboud@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: Katherine Green