Information Technology Laboratory Newsletter

Credit: Andrea Danti/Shutterstock

July—August 2013

Issue 124

INSIDE THIS ISSUE

NIST Reaches Out to the Private Sector for Assistance with Cybersecurity Framework for Critical Infrastructure

Under Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, NIST is directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure. Led by ITL, the framework will be developed by ongoing engagement with, and input from, stakeholders in government, industry, and academia, including an open public review and comment process, workshops, and other means of engagement.

Consistent with this approach, ITL recently held the second workshop on the development of the Cybersecurity Framework for Critical Infrastructure. The workshop brought together over 300 representatives from critical infrastructure owners and operators, industry associations, standards-developing organizations, and government to identify and achieve consensus on cross-sector principles, standards, guidelines, and practices that will be used to develop the initial draft framework.

Based on the current needs for the framework that have been identified through the Request for Information (RFI) responses, conclusions from the workshops, and NIST analysis, the Cybersecurity Framework will:

- Identify effective existing practices to inform an organization's risk management decisions related to the prevention and detection of, response to, and recovery from cybersecurity issues;
- Provide a modular and flexible approach to enable organizations to relate cybersecurity needs to diverse sector and organization mission/business drivers, and to be scalable and useful to organizations of varying sizes, business needs, and levels of maturity;
- Reinforce cybersecurity risk management as it relates to the mission and business risk management processes of an organization;
- Provide a means for an organization to express the maturity of their cybersecurity risk management practices to illustrate how those practices are integrated into the overall management processes of the organization;
- Include workforce considerations; and
- Address various types of dependencies, including those related to providers, processes, and technologies.

In several areas, ITL is seeking more information, including in the identification and availability of foundational cybersecurity practices, the actionable expression and management of privacy and civil liberties needs, and the availability of outcome-oriented metrics that leaders can use in evaluating the position and progress of the organization's cybersecurity status.

ITL will create an annotated outline of the draft Cybersecurity Framework, which will be available in late June 2013 on the framework website and will form the basis for discussion at the next workshop.

Credit: Kauffman/NIST

ITL's National Cybersecurity Center of Excellence Hosts Health Information Technology Mobile Device Use Case Meeting

The National Cybersecurity Center of Excellence (NCCoE) recently hosted a meeting to address a use case regarding the secure exchange of health information on mobile devices. This is the first use case in the project, "Secure Exchange of Electronic Health Information." The use case asks: How can the electronic exchange of test results, referrals, prescriptions, orders, and other information among healthcare providers and to patients on smart phones and tablet computers be made secure?

The NCCoE is a collaborative space where participants work with commercially available technologies to create solutions that can be rapidly applied to the cybersecurity challenges that businesses face each day. Solutions applicable to use cases and guidance on how to implement them are made publically available, and solutions are further refined with the help of feedback from their users.

Credit: Shutterstock

To kick off the Health IT Mobile Device Use Case project, the NCCoE recently hosted 35 representatives from 22 companies to familiarize them with the problem statement and the scope of work within the Cooperative Research and Development Agreement and to discuss which technological components they will contribute to the use case.

NIST Symposium Focuses on Developing and Evaluating Ontologies

NIST recently hosted a symposium on how to develop and evaluate "ontologies"—formal, computer-readable definitions of terms and their interrelationships —at its Gaithersburg campus. Titled "Ontology Evaluation across the Ontology Lifecycle," the workshop marked the end of four months of presentations and discussions that began in January 2013, held via the Internet and known as the Ontology Summit. Outputs of this collaborative event include:

- A Communique that provides the views and recommendations for proper ontology evaluation methods;
- A survey of software environments and tools to assess or promote the quality and fitness of ontologies;
- Results of seven hackathons addressing various evaluation and tool integration challenges; and
- An online growing collection of relevant literature.

The Ontology Summit provides the broader technical community a solid base for improving the quality of model-based systems. The website includes recordings of the entire series.

ITL-Organized Workshop Results in New 3D Shape Benchmark

A new 3D shape benchmark resulted from a conference track organized by ITL's Information Access Division researcher Afzal Godil. The track focused on Large-Scale Sketch-Based 3D Shape Retrieval in collaboration with Texas State University and the University of Konstanz in Germany. The objective of the sketch-based 3D model retrieval was to retrieve 3D models using a 2D sketch as input. This approach is intuitive and convenient for users to search for relevant 3D models and also important for several applications including sketch-based modeling and sketch-based shape recognition. The track was organized to foster this challenging research area by providing a common sketch-based retrieval dataset and soliciting retrieval results from current state-of-the-art retrieval methods for comparison. The new shape benchmark will provide a valuable contribution to the 3D shape retrieval and evaluation community.

Godil co-organized the Shape Retrieval Contest (SHREC) under the Eurographics Workshop on 3D Object Retrieval (3DOR'13). Four tracks were organized under SHREC; fourteen groups with 35 researchers from around the world participated in the 3D shape retrieval tracks and submitted 45 results based on different methods. The goals of the contest were to promote the development of shape retrieval methods and to evaluate and compare the effectiveness of different approaches. Papers on the shape contest were presented at the 3DOR'13, held in Gerona, Spain, on May 11, 2013.

Staff Recognition

At a recent InterNational Committee for Information Technology Standards (INCITS) Executive Board meeting, Michael Hogan and Elaine Newton, Office of the ITL Director, received the Chairman's Awards. This is an honorary award presented for providing outstanding service to the INCITS organization. The INCITS Chair selects the recipients. Michael Hogan was recognized for his advocacy of the advantages of placing standards work in INCITS and the International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1 on Information Technology (ISO/IEC JTC 1). Elaine Newton was recognized for her effective advocacy to protect the voluntary standards system from specific threats.

Michael Hogan (left) and Elaine Newton receive Chairman's Awards from Phil Wennblom, Intel.

Selected New Publications

Guidelines for Managing the Security of Mobile Devices in the Enterprise

By Murugiah Souppaya and Karen Scarfone
NIST Special Publication 800-124 Revision 1
June 2013

Mobile devices, such as smart phones and tablets, typically need to support multiple security objectives: confidentiality, integrity, and availability. To achieve these objectives, mobile devices should be secured against a variety of threats. The purpose of this publication is to help organizations centrally manage the security of mobile devices. Laptops are out of the scope of this publication, as are mobile devices with minimal computing capability, such as basic cell phones. This publication provides recommendations for selecting, implementing, and using centralized management technologies, and it explains the security concerns inherent in mobile device use and provides recommendations for securing mobile devices throughout their life cycles. The scope of this publication includes securing both organization-provided and personally owned (bring your own device, BYOD) mobile devices.

Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography

By Elaine B. Barker, Lily Chen, Allen Roginsky, and Miles Smid
NIST Special Publication 800-56A Revision 2
May 2013

This Recommendation specifies key-establishment schemes based on the discrete logarithm problem over finite fields and elliptic curves, including several variations of Diffie-Hellman and MQV key establishment schemes.

Guide to Industrial Control Systems (ICS) Security

By Keith A. Stouffer, Joseph Falco, and Karen Scarfone
NIST Special Publication 800-82 Revision 1
May 2013

This document provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

Glossary of Key Information Security Terms

Richard Kissel, Editor
NISTIR 7298 Revision 2
May 2013

The glossary provides a central resource of terms and definitions most commonly used in NIST information security publications and in the Committee for National Security Systems (CNSS) information assurance publications. The common security terms have been extracted from NIST Federal Information Processing Standards (FIPS), the Special Publication (SP) 800 series, NIST Interagency Reports (NISTIRs), and from the CNSS Instruction 4009 (CNSSI-4009). The NIST publications referenced are the most recent versions of those publications that were published prior to December 2012.

Incorporating Biometric Software Development Kits into the Development Process

By Karen Marshall, Ross J. Micheals, Kevin Mangold, and Kayee Kwong
NISTIR 7929
May 2013

The use of biometric devices has become critical to implementing various forms of security in a large number of organizations worldwide. The current state of biometric sensor integration is labor-intensive and prone to interoperability issues because of proprietary hardware and software, and a lack of standards in the Software Development Kit (SDK) installation process. Sensor integration incorporates the device hardware installation and intricate patchwork necessary to facilitate full communication between the device's software and the application that will ultimately command and control the target sensor. This document describes a process used to achieve more flexible and reliable integration of biometric sensor SDKs into the application development process.

Applied and Computational Sciences Division 2012 Annual Report

Ronald Boisvert, Editor
NISTIR 7931
May 2013

This report summarizes the technical work of the Applied and Computational Sciences Division of NIST's Information Technology Laboratory. Part I, Overview, provides a high-level overview of the Division's activities, including highlights of technical accomplishments during the previous year. Part II, Features, provides further details on ten projects of particular note this year. This is followed in Part III, Project Summaries, by brief synopses of all technical projects active during the past year. Part IV, Activity Data, provides listings of publications, technical talks, and other professional activities in which Division staff members participated. The reporting period covered by this document is October 2011 through December 2012.

Upcoming Technical Conferences

3rd Cybersecurity Framework Workshop
Dates and Place: July 10-12, 2013, at the University of California, San Diego (UCSD), La Jolla, California
Sponsors: NIST, UCSD, and the National Health Information Sharing and Analysis Center (NH-ISAC)
Cost: None

At this workshop, NIST will present an annotated outline of the initial draft Cybersecurity Framework for discussion. Participants are asked to review posted materials (available on the conference website by June 28, 2013) prior to arrival at the workshop and to come prepared to offer substantive input on the level of guidance, integration with existing standards, practices, and guidelines, and potential gaps.
NIST contact: Suzanne Lightman, suzanne.lightman@nist.gov

2013 Biometric Consortium Conference & Biometric Technology Expo
Dates and Place: September 17-19, 2013, Tampa Convention Center, Tampa, Florida
Sponsors: NIST, National Security Agency, and AFCEA International
Cost: $595 - $695

The Biometric Consortium Conference will focus on biometric technologies for defense, homeland security, identity management, border crossing, and electronic commerce. The conference will feature four tracks, including the AFCEA Identity Management (IdM) track, panel discussions, workshops, and a biometrics tutorial. The keynoter will be Jeremy Grant, Senior Executive Advisor for Identity Management, National Strategy for Trusted Identities in Cyberspace (NSTIC), Information Technology Laboratory, NIST.
NIST contact: Fernando Podio, fernando.podio@nist.gov

The Intersection of Cloud and Mobility
Dates and Place: October 1-3, 2013, NIST, Gaithersburg, Maryland
Sponsor: NIST
Cost: None

As part of its continuing cloud computing series, NIST/ITL is hosting a new forum on Cloud and Mobility. Join experts in the fields of cloud, mobility, and measurement for thought-provoking plenary talks, panel presentations, facilitated breakout discussion, poster sessions, and networking around these themes: Federal Perspectives on Cloud and Mobility; The Vision for Cloud and Mobility; Current State of Cloud and Mobility Intersections; Intersections of Cloud and Mobility on the Horizon; Bringing Mobility and Cloud Together; Challenges and Lessons Learned; Path Forward to a Federated Mobile Cloud; Lessons Learned in Mobility; and Challenges for Cloud and Mobility.
NIST contacts: Michaela Iorga, michaela.iorga@nist.gov; Frederic de Vaulx, frederic.devaulx@nist.gov

Fundamentals of Uncertainty Analysis
Dates and Place: October 22-24, 2013, NIST, Gaithersburg, Maryland
Sponsor: NIST
Cost: $1275

This short course covers many aspects of the propagation of uncertainty using the methods outlined in the JCGM Guide to the Expression of Uncertainty in Measurement. Exercise and hands-on applications will use functions for uncertainty analysis from the free software package, metRology, written for the open source R statistical computing environment. The functions will be accessed via an Excel graphical user interface that is available as a free add-in.
NIST contact: Will Guthrie, william.guthrie@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 NIST campus in Gaithersburg, Maryland.

Credit: NIST

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