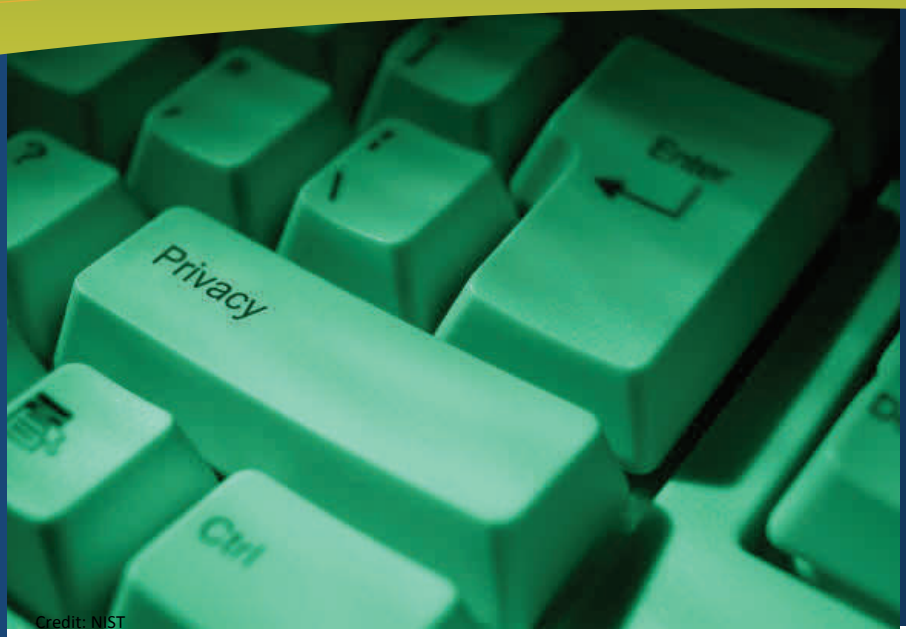
Information Technology Laboratory Newsletter

INSIDE THIS ISSUE





Credit: NIST

May-June 2014

Issue 129

# ITL Focuses on Privacy Challenges

Privacy is a challenging subject that spans a number of domains, including law, policy and technology. Notwithstanding numerous sets of principles, including the foundational Fair Information Practice Principles (FIPPs), that seek to address the handling of individuals' personal information, many concerns exist about the future of privacy in the face of rapidly evolving technologies. Process-oriented principles are an important component of an overall privacy framework, but on their own, they do not achieve consistent and measurable results in privacy protection. In the security field, risk management models, along with technical standards and best practices, are key components of security frameworks. To date, the privacy field has lagged behind in the development of analogous components.

To address these gaps and challenges, and in support of the activities set forth in Section 4.9 of the NIST Roadmap for Improving Critical Infrastructure Cybersecurity (developed pursuant to Executive Order 13636), ITL hosted a Workshop on Privacy Engineering on April 9-10, 2014, at the Gaithersburg campus. The workshop focused on the advancement of privacy engineering as a basis for the development of technical standards and best practices for the protection of individuals' privacy or civil liberties.

Over 240 participants from the private sector, academics, government, and the privacy and civil liberties community participated on-site in discussions on privacy harms, data actions, and use cases. In addition to on-site participants, over 100 people joined to view the live webcast of panels and presentations on the current state of privacy engineering. Meeting participants discussed the gap that exists between the discussions of privacy at the policy level and the implementation of privacy protections at the system level. There was general agreement that better tools, practices, and even vocabulary are needed to fill that gap. For more information, see the workshop presentations.

Based on these discussions and presentations, ITL is planning a privacy engineering initiative that will concentrate on developing reusable tools and practices to facilitate the creation and maintenance of systems with strong privacy postures. This initiative will solicit the contributions of a variety of communities including privacy and civil liberties, system engineering, private sector management, academics, and government.

## ITL's Static Analysis Tool Evaluation Advances

ITL's Software Assurance Metrics and Tool Evaluation (SAMATE) team advanced their work on the Static Analysis Tool Exposition (SATE) with a fifth round of tool analysis (SATE V). Similar to the previous four SATE efforts, SATE V consisted of ITL scientists choosing a suite of programs, participating static analysis tool makers running their tools on the suite, then ITL scientists analyzing the tool reports. For SATE V, the set of programs consisted of five large open source programs selected for having known (CVE-reported) vulnerabilities and also 90,000 synthetic test cases in C/C++ and JAVA known as the Juliet test suite. A record number of static analysis tools, 14, were run on the test set. SATE V culminated in a workshop where participants and organizers of SATE gathered to share their experiences, report interesting observations, and discuss lessons learned. Some 65 people attended from around the world. The workshop began with the SAMATE team announcing the new name for their massive public repository of programs with known vulnerabilities: Software Assurance Reference Dataset or SARD. In addition to presentations by six participating tool makers, ITL scientists reported their preliminary observations and findings. The workshop concluded with a feedback session focused on the planning of SATE VI.

Tool vendors applauded several improvements over the previous SATE. Participants appreciated the SAMATE team's careful preparation, triage, and analysis. They found that having a common set of test cases allowed them to confirm tool coverage, offer baselines for accuracy and performance, provide repeatable results, and reassure their customers. Many tool makers plan to use the SATE test cases to refine their tools in their internal nightly testing. Others reported that SATE participation encouraged enhanced functionality and enlarged code capacity to encompass this year's test cases.

Participants also suggested future improvements and research directions; many observed that uniformity in reporting remains a challenge. Tool makers look to the SAMATE team for greater clarity in classes of software bugs so the tools can provide better reporting and remediation recommendations. Comments from attendees illustrated the growing customer interest in detecting and eradicating software weaknesses before deployment.

## ITL Promotes Healthcare Interoperability

ITL participated in the 2014 Connectathon held in Chicago, one of three events held annually in North America, Europe, and Asia. The major goal of the Connectathon is to promote the adoption of standards-based interoperability solutions defined by Integrating the Healthcare Enterprise (IHE) in commercially available healthcare IT systems. The Connectathon, the Health Information Technology (IT) industry's largest interoperability testing event, serves as an industry-wide testing event where developers of health information systems can test their implementations with those of other vendors.

The North American Connectathon in Chicago featured more than 140 systems from over 97 participating organizations, and more than 3800 successful tests of IHE Integration Profiles were performed and verified. In addition to nearly 500 systems engineers engaged in testing at the event, more than 100 attendees took part in a conference featuring prominent speakers on health IT and electronic health records. Ninety percent of the participants at the event used NIST tooling, provided and verified by ITL scientists, who also served as Connectathon monitors to verify test results on the show floor.

Results of the Connectathon are published in the IHE Product Registry. This is a searchable database of IHE Integration Statements (conformance to IHE Profiles tested) as published by vendors with IHE capabilities in their product offerings.

## Cloud and Mobility Intersect at ITL Workshop


ITL recently hosted the Intersection of Cloud and Mobility Forum and Workshop .The event, the seventh in the series, offered a vast platform for information sharing and networking to over 360 cloud and mobility experts. The forum and workshop included exhilarating plenary sessions, thought-provoking panel discussions, and dynamic brainstorming breakout sessions focused on topics such as a future vision for the intersection of cloud and mobility; the current state of the cloud and mobility; challenges encountered; and the roadmap to an enhanced mobile cloud. All plenary sessions and panels were broadcast, and the recordings can be found at this website. Additionally, all visual materials (e.g., presentations) are available for review and/or download at this website.

## Staff Recognition

Two ITL staffers recently received 2014 Federal 100 awards:

- Senior Privacy Policy Advisor Naomi Lefkovitz was recognized for her efforts to safeguard privacy in the identity-management initiative being developed via the National Strategy for Trusted Identities in Cyberspace.

- Matthew Scholl, Acting Chief, Computer Security Division, was honored for his role in directing the new Cybersecurity Framework, NIST's actions in response to the Digital Government Strategy, and the cross-agency priority goal on cybersecurity.

The Federal 100 are chosen by government and industry leaders convened by the magazine Federal Computer Week as a list of federal employees whose work has significantly advanced federal IT in the past year.

## Selected New Publications

[A Methodology for Developing Authentication Assurance Taxonomy for Smart Card-Based Identity Verification]
By Ramaswamy Chandramouli
NISTIR 7849
March 2014

Smart cards (smart identity tokens) are now being extensively deployed for identity verification for controlling access to IT resources as well as physical resources. Depending upon the sensitivity of the resources and the risk of wrong identification, different authentication use cases are being deployed. Assignment of authentication strength for each of the use cases is often based on: (a) the total number of three common orthogonal authentication factors – What You Know, What You Have and What You are; and (b) the entropy associated with each factor chosen. The objective of this paper is to analyze the limitation of this approach and present a methodology for assigning authentication strengths based on the strength of pair wise bindings between the five entities involved in smart card based authentications – the card (token), the token secret, the card holder, the card issuer, and the person identifier stored in the card.

[Examination of the Impact of Fingerprint Spatial Area Loss on Matcher Performance in Various Mobile Identification Scenarios]
By Shahram Orandi, Kenneth Ko, Stephen S. Wood, John D. Grantham, and Michael Garris
NISTIR 7950
March 2014

NIST conducted a study of the FBI Repository for Individuals of Special Concern (RISC) system using various gallery and Mobile ID [MOBID] acquisition profile combinations to examine performance characteristics of the various profiles in terms of matching effectiveness and throughput. Results of the study showed that the predominant RISC operational case of Mobile ID FAP10 (fingerprint acquisition profile 10) using the left and right index fingers is at a marked disadvantage in terms of matcher performance compared to the larger FAP20 and FAP30 cases using the same fingers. Conclusion: System false non-identification rates suffer a significant performance penalty in the typical operational case of FAP10 two index finger (2,7) capture.

[Towards NFIQ II Lite: Self-Organizing Maps for Fingerprint Image Quality Assessment]
By Elham Tabassi
NISTIR 7973
February 2014

Fingerprint quality assessment is a crucial task which needs to be conducted accurately in various phases in the biometric enrolment and recognition processes. We propose a computationally efficient means of predicting biometric performance based on a combination of unsupervised and supervised machine learning techniques. We train a self-organizing map (SOM) to cluster blocks of fingerprint images based on their spatial information content. The output of the SOM is a high-level representation of the finger image, which forms the input to a random forest trained to learn the relationship between the SOM output and biometric performance. The quantitative evaluation demonstrates that our proposed quality assessment algorithm is a reasonable predictor of performance.

[IREX IV: Part 2, Compression Profiles for Iris Image Compression]
By George W. Quinn, Patrick J. Grother, and Meilee L. Ngan
NISTIR 7978
January 2014

The IREX IV evaluation builds upon IREX III as a performance test of one-to-many iris recognition. This report is the second part of the IREX IV evaluation, which specifically evaluates the ability of automated iris recognition algorithms to match heavily compressed standard iris images and determines the optimal set of compression parameters for JP2 compression and the maximum capabilities for one-to-many matching.

[Report: Authentication Diary Study]
By Michelle P. Steves
NISTIR 7983
February 2014

Users have developed various coping strategies for minimizing or avoiding the friction and burden associated with managing and using their portfolios of user IDs and passwords or personal identification numbers (PINs). Many try to use the same password (or different versions of the same password) across different systems. Others use memory aids or technological assistants such as password management software. We were interested in these coping strategies and the friction points that prompt people to use them. More broadly, we wanted to address a pressing research need by gathering data for user-centered models of how people interact with security as part of their daily life, as empirical research in that area is currently lacking.

[Integrating Electronic Health Records into Clinical Workflow: An Application of Human factors Modeling Methods to Ambulatory Care]
By Svetlana Lowry, Mala Ramaiah, E.S. Patterson, D. Brick, A.P. Gurses, A. Ozok, and M.C. Gibbons
NISTIR 7988
March 2014

The recommendations in this report provide a first step in moving from a billing-centered perspective (i.e., focusing on ensuring maximum and timely reimbursement) to a clinician-centered perspective where the electronic health record design supports clinical cognitive work. These recommendations point the way towards a “patient visit management system,” which incorporates broader notions of supporting workload management, supporting the flexible flow of patients and tasks, and preventing common workarounds.

[United States Federal Employees’ Password Management Behaviors – a Department of Commerce Case Study]
By Yee-Yin Choong, Mary Theofanos, and Hung-Kung Liu
NISTIR 7991
April 2014

We designed an on-line survey to collect data on end-users’ password management and their attitudes toward computer security in a government work environment. This paper focuses on the data collected from employees of the Bureaus of the U.S. Department of Commerce between June 2010 and June 2011.

.

# Upcoming Technical Conferences

IT Professional Conference: Challenges in Information Systems
Date: May 22, 2014
Place: NIST, Gaithersburg, Maryland
Sponsors: NIST and IEEE Computer Society
Cost: None

This conference, organized by IEEE IT Professional magazine, seeks to bring together IT professionals and managers from industry, government, and academia to examine the new challenges facing Information Systems, and to explore how they can be successfully addressed.
NIST contact: Richard Kuhn

Int'l. Workshop on Enabling Science from Big Image Data
Date: May 27-31, 2014
Place: Stanford, California
Primary sponsor: Academy of Science and Engineering (ASE)
Cost: Variable

The workshop brings together the community working on a specific image type of Big Data. Image Big Data have characteristics that can be leveraged in tackling the overarching challenges of Big Data. The workshop would be of interest to all scientific areas that conduct their domain-specific science by (a) acquiring images via measurement instruments that form raster data (e.g., microscopes, video cameras, scanners, telescopes); and (b) analyzing large volumes of image data to discover spatial, temporal, and spectral relationships that require large global and precise local information.
NIST contact: Peter Bajcsy

NIST Mobile Forensics Workshop and Webcast
Date: June 18, 2014
Place: NIST, Gaithersburg, Maryland
Sponsors: ITL and NIST Law Enforcement Standards Office
Cost: None

This workshop will explore the latest technology advancements and applications in mobile device forensics. It will educate attendees on the latest developments in the forensic analysis of mobile devices and how technologies are used in casework. The information provided will increase the situational awareness of investigators and criminal justice stakeholders across the United States about the latest trends, analysis protocols, and issues encountered when applying analysis tools to mobile devices.
NIST contact: Richard Ayers

SHA-3 2014 Workshop
Date: August 22, 2014
Place: University of California, Santa Barbara, California
Sponsor: NIST
Cost: TBD

The goal of the workshop is for the community to help NIST get a better understanding of SHA-3 and its possible applications, with particular focus on additional modes of operation for SHA-3 that might be worth standardizing in the future.
NIST contact: Shu-jen Chang



The NIST campus in Gaithersburg, Maryland.

Credit: Katherine Green

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