Information Technology Laboratory Newsletter

February 2012

Issue 117

INSIDE THIS ISSUE

ITL Welcomes Charles Romine As New Director

On November 21, 2011, ITL welcomed as it new director Charles (Chuck) H. Romine. Romine has previously served as NIST's Acting Associate Director for Laboratory Programs, Senior Policy Advisor to the NIST Director, and as ITL's Associate Director for Program Implementation. He joined NIST in 2009 after serving for five years in the White House Office of Science and Technology Policy as Senior Policy Analyst for Information Technology. As ITL Director, Romine oversees a research program designed to promote U.S. innovation and industrial competitiveness by developing and disseminating standards, measurements, and testing for interoperability, security, usability, and reliability of the nation's information systems.

ITL Publishes Revised Biometrics Standard

The ANSI/NIST-ITL standard, *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information*, has been revised as ANSI/NIST-ITL 1-2011 and published as NIST Special Publication 500-290, superseding all previous versions and amendments to the standard. Law enforcement, intelligence community, military and homeland security organizations around the world rely upon the ANSI/NIST-ITL standard in order to exchange biometric information. All agencies transmitting fingerprint, palmprint, facial images/mugshots, scar, marks, tattoos (SMT), iris, and other biometric images and related data to the FBI must adhere to the format described by this ANSI/NIST-ITL standard.

ITL serves as the standards development organization (SDO) for this standard; Bradford J. Wing served as editor of the standard. In 2010, ITL held two workshops with participation from federal, state, and local government agencies, foreign governments, international organizations (such as INTERPOL), academia, and private industry to address proposed additions and revisions to the standard. Sixteen working groups established at the first workshop prepared the content for the revised standard. The ANSI/NIST-ITL standard ballot to approve the revised standard closed on November 9, 2011, and was passed unanimously. See the new standard here.

ITL Releases Prototypes and Test Tools for Internet Routing Security

ITL recently demonstrated the first open source prototypes of emerging security extensions to the Internet's Border Gateway Protocol (BGP). The NIST prototype, BGP Secure Routing eXtension (BGP-SRx), is an open source reference implementation and research platform for investigating emerging BGP security extensions and supporting protocols. For more information on BGP-SRx and to download the prototype and tools, see here.

To facilitate remote testing of commercial BGP security implementations and supporting public key infrastructures, ITL released the BRITE (BGPSEC/RPKI Interoperability Test & Evaluation) system. BRITE, an online distributed interoperability test system developed and hosted at NIST, allows router vendors and Internet Service Providers (ISPs) to test and evaluate all of the protocols and algorithms required by emerging Internet Engineering Task Force (IETF) BGP security solutions. For more information on BRITE or to use the remote test system, see here.

ITL Advances Federal Cloud Computing Initiative

Through its recent fourth public Cloud Computing forum and workshop, ITL expanded the collaborative development of standards, explored cloud-related technical concepts, issues and solutions, and served as a calibration point for NIST to integrate its work with the broader Cloud Computing community. The workshop introduced NIST Special Publication 500-293, Draft *U.S. Government Cloud Computing Technology Roadmap*. The roadmap is a vehicle to define and communicate prioritized interoperability, portability, and security requirements that must be met in order to accelerate secure and effective U.S. government (USG) Cloud Computing deployment.

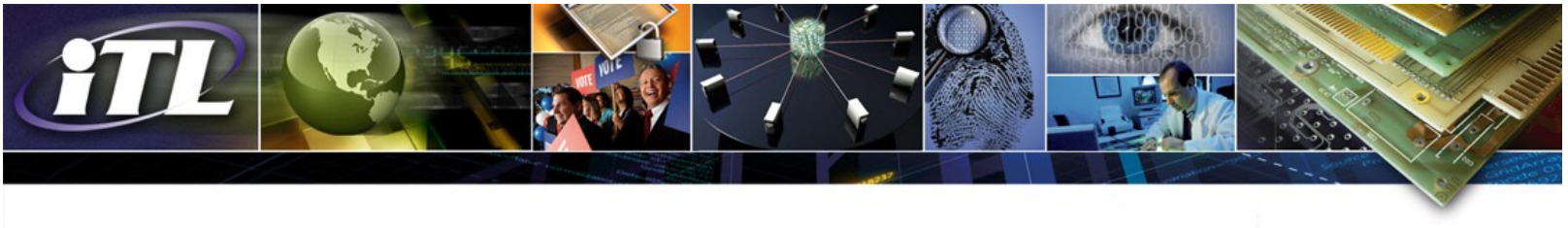
ITL researchers Murugiah Souppaya, Lee Badger, and Larry Keys investigate security techniques for protecting virtualized computing environments and cloud computing systems. His virtualization lab serves as a testbed to develop and implement controls that reduce security vulnerabilities and minimize exposure to cyber attacks, and also provides virtualized computing services for other ITL research projects.

ITL has a technology leadership role in support of USG adoption of the Cloud Computing model to reduce costs and improve the ability to quickly create and deploy enterprise applications. NIST plays a central role in defining and advancing standards, and collaborating with U.S. government agency Chief Information Officers, private sector experts, and international bodies to identify and reach consensus on Cloud Computing technology and standardization priorities. More information is available through the ITL Cloud Computing website, here. Public stakeholder participation in the collaborative roadmap development is encouraged. All parties are invited to register as public working group members, and to directly contribute through the NIST ITL Cloud Computing collaboration website here.

ITL Improves Health Information Technology Testing Toolkit

A recent ITL workshop focused on improvements to the healthcare toolkit, a NIST-developed software platform for developing and executing health information technology system-related tests focusing on both conformance and interoperability styles of testing. The toolkit has been used for the last two years in North America and Europe as part of the testing program defined by Integrating the Healthcare Environment (IHE). It is also used by the Office of the National Coordinator for Health Information Technology and their contractors as part of their Nationwide Health Information Network (NwHIN) initiative.

The ITL workshop was attended by developers from NIST, industry, and university settings from the United States and Europe. The technical focus of the workshop was to enable developers to create new tests as well as add extensions to the basic toolkit infrastructure for their testing needs. Based on the feedback and attendance, future workshops will be offered. See here.



Selected New Publications

Report on the Third Static Analysis Tool Exposition (SATE2010)
By Vadim Okun, Paul Black, and Aurelien Delaitre
NIST Special Publication 500-283
November 2011

The NIST Software Assurance Metrics And Tool Evaluation (SAMATE) conducted the third Static Analysis Tool Exposition (SATE) in 2010 to advance research in static analysis tools that find security defects in source code. This document describes the SATE procedure and provides observations based on the data collected.

Recommendation for Key Derivation through Extraction-then-Expansion
By Lily Chen
NIST Special Publication 800-56C
November 2011

This recommendation specifies techniques for the derivation of keying material from a shared secret established during a key establishment scheme defined in NIST Special Publications 800-56A or 800-56B through an extraction-then-expansion procedure.

Electronic Authentication Guideline
By William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, and Emad A. Nabbus
NIST Special Publication 800-63-1
December 2011

This recommendation provides technical guidelines for federal agencies implementing electronic authentication and is not intended to constrain the development or use of standards outside of this purpose. The recommendation covers remote authentication of users interacting with government IT systems over open networks. It defines technical requirements for each of four levels of assurance in the areas of identity proofing, registration, tokens, management processes, authentication protocols and related assertions.

Recommendation for Existing Application-Specific Key Derivation Functions
By Quynh H. Dang
NIST Special Publication 800-135, Rev. 1
January 2012

Cryptographic keys are vital to the security of Internet security applications and protocols. Many widely used Internet security protocols have their own application-specific Key Derivation Functions (KDFs) that are used to generate the cryptographic keys required for their cryptographic functions. This recommendation provides security requirements for those KDFs.

Integrating jQuery with the 3D Descriptive Markup of X3DOM
By Sanford P. Ressler
NISTIR 7827
October 2011

This paper describes a number of techniques using jQuery to take advantage of the 3D descriptive markup implemented by X3DOM. Given 3D descriptive markup, this paper demonstrates a number of techniques that take advantage of having the 3D geometry and scene graph represented directly in a web browser. Placing a 3D scene graph into the browsers DOM (Document Object Model) offers the opportunity to leverage frameworks such as jQuery in powerful ways.

Ocular and Iris Recognition Baseline Algorithm
By Yooyoung Lee, Ross Micheals, James Filliben, Jonathon Phillips, and Hassan Sahibzada
NISTIR 7828
November 2011

Due to its distinctiveness, the human eye is a popular biometric feature used to identity a person with high accuracy. The “Grand Challenge” in biometrics is to have an effective algorithm for subject verification or identification under a broad range of image and environmental conditions. As a response to the challenge, this paper presents baseline performance results derived from an enhanced version of VASIR (Video-based Automated System for Iris Recognition), as well as initial performance results based on a broader ocular recognition system.

Performance of Face Recognition Algorithms on Compressed Images
By George Quinn and Patrick Grother
NISTIR 7830
November 2011

This report provides a comprehensive assessment of the ability of face recognition algorithms to compare compressed standard face images. Six well-performing algorithms from the Multiple Biometric Evaluation (MBE) 2010 Still Face Track are used to compare face images compressed in JPEG and JPEG2000 formats. A primary goal is to identify the maximum storage constraints under which verification systems can effectively operate. Toward this end, we provide guidelines and recommendations for the efficient compression and storage of face images for biometric applications.

Selected New Publications

Initiating Mobile Software Development – Lessons Learned From a 12-Month Project

By Frederic de Vaulx, Paul Khourisaba, Marcus Newrock, and Bertrand Stivalet
NISTIR 7838
January 2012

As mobile devices capabilities keep on improving, today's mobile software ecosystem evolves at an unprecedented speed. This evolution makes mobile software development more common and critical. Moreover, the ever-increasing number of new development platforms can make it difficult for developers new to mobile application development. Are there elements developers can leverage in order to create what is good quickly and successfully? In the article, we explore what we found to be a set of key elements to building our applications and optimizing our development process.

Upcoming Technical Conferences

2012 NIST/NSTIC IDtrust Workshop
Dates: March 13-14, 2012
Place: NIST, Gaithersburg, Maryland
Sponsors: NIST and OASIS ID Trust Member Section
Fee: $148

With the theme of Technologies and Standards Enabling the Identity Ecosystem, the workshop will focus on how technologies and standards can help the framework of the identity ecosystem coalesce. The workshop will feature plenary presentations and panel discussions by leading identity management and standards experts addressing a broad swath of technology and standards issues that surround identifying and implementing the four NSTIC Guiding Principles in the Identity Ecosystem: Identity Solutions will be Privacy-Enhancing and Voluntary; Identity Solutions will be Secure and Resilient; Identity Solutions will be Interoperable; and Identity Solutions will be Cost-Effective and Easy To Use.

NIST contact: Sara Caswell, 301/975-4632
email: sara.caswell@nist.gov

Third Secure Hash Algorithm (SHA-3) Candidate Conference
Dates: March 22-23, 2012
Place: Washington Marriott Hotel, Washington, D.C.
Sponsor: NIST
Fee: $490 ($390 students)

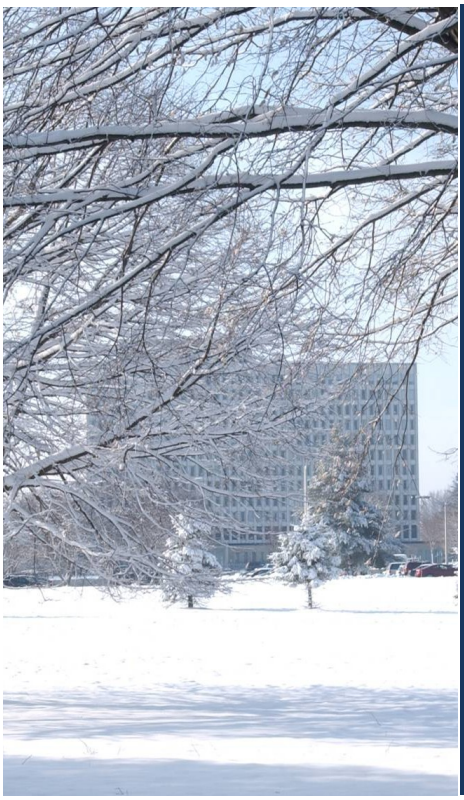
The purpose of the conference is to discuss the SHA-3 finalist algorithms, and to solicit public feedback before NIST selects a winning algorithm for standardization later in 2012.

NIST contact: Shu-jen Chang, 301/975-2940
email: shu-jen.chang@nist.gov

Federal Information Systems Security Educators' Association (FISSEA) Conference
Dates: March 27-29, 2012
Place: NIST, Gaithersburg, Maryland
Sponsors: FISSEA and NIST
Fee: $165

The conference theme is A New Era in Cybersecurity Awareness Training and Education. Tracks and presentations will focus on current projects, emerging trends, and initiatives in cybersecurity awareness, training, and education.

NIST contact: Peggy Himes, 301/975-2489
email: peggy.himes@nist.gov



If you are interested in receiving our newsletter, send your name, organization, and business mailing address to:

ITL Newsletter
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900

You will be placed on this mailing list only.

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of new information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our Web site is 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
E-mail: elizabeth.lennon@nist.gov

TO SUBSCRIBE TO THE ELECTRONIC EDITION OF THE ITL NEWSLETTER, GO TO ITL HOMEPAGE

NIST/Denease Anderson