

ITL NEWSLETTER FOR NOVEMBER 2009

ITL SEEKS COMMENTS ON IPv6 TESTING PROGRAM

As part of the federal government transition from Internet Protocol (IP) v4 to IPv6, ITL has developed a testing program of the new protocol and announces a 30-day public review and comment period prior to the initiation of the testing program. **Comments are due November 14, 2009**, and may be made via the following Web site: <http://w3.antd.nist.gov/usgv6/testing.html>. This Web site presents all related publications and background information. We invite your participation in this process.

The IPv6 Testing Program comprises standardized test suites for interoperability and conformance, and laboratories that are accredited to execute those test methods. Issued in September 2009, NIST Special Publication (SP) 500-273, *IPv6 Test Methods: General Description and Validation*, by Stephen Nightingale, specifies the validation requirements for test methods and test specifications used to test host, router, and network protection devices required by the U.S. government profile for IPv6. As a prudent step to secure procedurally correct testing, ITL is recommending that testing be done in laboratories accredited to ISO 17025. That standard refers to general testing requirements, and NIST SP 500-273 specifies the technical test methods involved in IPv6 device testing. This embraces both the conduct of each type of testing and the validation of test methods.

The bedrock of each testing framework is a set of published test specifications, traceable to the protocol specifications. Abstract Test Specifications are initially validated against protocol specifications or standards. This process gives some confidence in the integrity of the Abstract Test Specifications so that executable test methods can be validated by the laboratory, against these abstract test procedures. Conformance, Interoperability and network protection device testing have different traceability chains, and these are further detailed in the document. Tests, like software, are always works in progress. In continuous operation there will be bugs, and confusions of interpretation. In order to converge on a truly interoperable community, it is necessary that tests be maintained in synchronization across all participating laboratories, and test interpretations be agreed among laboratories and test method suppliers. We welcome your comments and suggestions as we continue to refine our IPv6 testing program.

ITL Publishes Best Practices for Mobile ID Fingerprint Capture

Mobile ID devices allow first responders, law enforcement agents, and soldiers to collect biometric data in remote locations, and either compare them with other samples contained in a database on that device or transmit the data for comparison with samples in a central repository. A new ITL publication, NIST Special Publication 500-280, *Mobile ID Device Best Practice Recommendation, Version 1.0*, presents a community-developed series of guidelines that, if followed, will provide the required levels of interoperability for various operational scenarios. Written by Shahram Orandi and R. Michael McCabe, the Mobile ID Best Practices Recommendation (BPR) is also addresses intrinsic limitations of handheld devices by allowing specific mitigation strategies. The

new publication is available at <http://fingerprint.nist.gov/mobileid/MobileID-BPRS-20090825-V100.pdf>.

Currently, most biometrically enabled law enforcement applications call for the capture of fingerprints from all ten fingers of an individual. This is made easy by the fact that desktop fingerprint scanners provide a large platen (scanning area) that can be used to capture all ten fingers in a fast three-step process (right four fingers together, left four fingers together, and both thumbs together). Most portable devices, however, have platens that are a fraction of the size of a desktop-size scanner. The Mobile ID BPR provides guidelines that allow for the capture of all ten fingerprints on a scanner with a smaller platen using a two-fingers-at-a-time approach.

ITL has been involved in the field of biometric identification since the late 1960s. Part of this involvement has been with the creation of standards for collection and transmission of biometric data to ensure interoperability between all identification/verification systems. Until recently, this work has been primarily focused on stationary/desktop capture environments with hard-wired processing pathways. Recently, however, the proliferation of miniaturized devices such as advanced PDAs and ultra-portable personal computers as well as high-speed cellular networks has made portable biometric systems a reality. While the capabilities of these portable systems have increased dramatically, they still have intrinsic limitations that must be overcome to ensure interoperability with their larger, more established desktop environments. This ITL biometrics project was funded by the Federal Bureau of Investigation.

ITL Strives to Improve the Information Security of Small Businesses

With small businesses being a vital component of the U.S. economy, it is critical that they consider information security as a priority. To assist with this, ITL has developed guidelines for small businesses to improve the security of their information technology. NISTIR 7621, *Small Business Information Security: The Fundamentals*, by Richard L. Kissel, will assist small business management in understanding how to provide basic security for their information, systems, and networks. The document is available at <http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf>. See also the NIST video on small business information security at http://www.nist.gov/public_affairs/techbeat/tb2009_1006.htm#small.

ITL Explores End-to-End Voting Systems

ITL recently sponsored an End-to-End Voting System Workshop at George Washington University in Washington, D.C. An end-to-end voting system is one which enables voter verification of the outcome of the election. The workshop brought together researchers in cryptography, security, and usability, and election practitioners including election officials and voting system manufacturers, to explore the security and usability properties of this type of innovative voting system. More than 60 participants from the United States, Canada, Germany, Belgium, Australia, Poland, and the United Kingdom attended the event. The workshop covered a wide range of topics that impact end-to-end voting systems including usability, security, desired properties, and tradeoffs between different types of implementations. The final panel explored what the next steps should be to

advance end-to-end voting systems including needed research, pilots, and standardizations. The Web site is <http://vote.nist.gov>.

SELECTED NEW PUBLICATIONS

Recommendation for EAP Methods Used in Wireless Network Access Authentication

By Katrin Hoepfer and Lily Chen

NIST Special Publication 800-120

September 2009

<http://csrc.nist.gov/publications/nistpubs/800-120/sp800-120.pdf>

This Recommendation specifies security requirements for authentication methods with key establishment supported by the Extensible Authentication Protocol (EAP) defined in IETF RFC 3748 for wireless access authentications to federal networks.

Recommendation for Digital Signature Timeliness

By Elaine Barker

NIST Special Publication 800-102

September 2009

<http://csrc.nist.gov/publications/nistpubs/800-102/sp800-102.pdf>

Establishing the time when a digital signature was generated is often a critical consideration. A signed message that includes the (purported) signing time provides no assurance that the private key was used to sign the message at that time unless the accuracy of the time can be trusted. With the appropriate use of digital signature-based timestamps from a Trusted Timestamp Authority (TTA) and/or verifier-supplied data that is included in the signed message, the signatory can provide some level of assurance about the time that the message was signed.

Directions in Security Metrics Research

By Wayne Jansen

NISTIR 7564

August 2009

http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf

During the last few decades, researchers have made various attempts to develop measures and systems of measurement for computer security with varying degrees of success. This paper provides an overview of the security metrics area and looks at possible avenues of research that could be pursued to advance the state of the art.

Assessing Face Overlay

By Mary Theofanos, Brian Stanton, Charles Sheppard, Ross Micheals, Yee-Yin Choong, John Wydler, Kevin Mangold, Michelle Potts Steves, and Emile Morse

NISTIR 7578

May 2009

http://zing.ncsl.nist.gov/biousa/docs/face_overlay_report_final_approved.pdf

The U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program has embarked on an effort to improve the quality of facial images captured at U.S. ports of entry. One aspect of this effort is the identification of usability and human factors issues that may impact face image capture. This report describes a usability test that assessed the use of a face overlay guide to assist the camera operator center and align the face image.

Estimating Volumes of Simulated Lung Cancer Nodules

By David Gilsinn, Bruce Borchardt, and A. Tebbe

NISTIR 7571

July 2009

david.gilsinn@nist.gov

The Food and Drug Administration (FDA) is conducting research on developing reference cancer lesions, called phantoms, to test CT scanners and their proprietary software. FDA loaned two semi-spherical phantoms to NIST, called Green and Pink, and asked to have the phantoms measured by a coordinate measuring machine (CMM) and the volumes estimated. This report describes both the experimental and computational methods used to estimate the phantoms' volumes as well as a bootstrap method for estimating the uncertainties of the computed volumes.

System and Network Security Acronyms and Abbreviations

By Karen Scarfone and V. Thompson

NISTIR 7581

September 2009

<http://csrc.nist.gov/publications/nistir/ir7581/nistir-7581.pdf>

This report contains a list of selected acronyms and abbreviations for system and network security terms with their generally accepted or preferred definitions. It is intended as a resource for federal agencies and other users of system and network security publications.

Guidelines for Writing Clear Instructions and Messages for Voters and Poll Workers

By Janice Redish and Sharon Laskowski

NISTIR 7596

June 2009

<http://vote.nist.gov/032906PlainLanguageRpt.pdf>

This handbook presents guidelines for clear ballot instructions for both paper and electronic ballots. It also gives guidance on writing clear system messages on electronic voting machines.

Overview of the Multiple Biometrics Grand Challenge

By P. Jonathon Phillips, Patrick J. Flynn, J. Ross Beveridge, W. Todd Scruggs, Alice J. O'Toole, David Bolme, Kevin W. Bowyer, Bruce A. Draper, Geof H. Givens, Yui Man Lui, Hassan Sahibzada, Joseph A. Scallan III, and Samuel Weimer

NISTIR 7607

August 2009

http://www.nd.edu/~kwb/PhillipsEtAlICB_2009.pdf

The goal of the Multiple Biometrics Grand Challenge (MBGC) is to improve the performance of face and iris recognition technology from biometric samples acquired under unconstrained conditions. The MBGC is organized into three challenge problems: the portal challenge problem, the still face challenge problem, and the video challenge problem. Each challenge problem relaxes the acquisition constraints in different directions. All three challenge problems include a large data set, experiment descriptions, ground truth, and scoring code.

IREX I: Performance of Iris Recognition Algorithms on Standard Images

By Patrick Grother, Elham Tabassi, George Quinn, and Wayne Salamon

NISTIR 7629

September 2009

http://iris.nist.gov/irex/irex_summary.pdf

The Iris Exchange (IREX) was initiated by NIST in late 2007 to support interoperable exchange of iris imagery in high performance biometric applications. The first activity in the program, the IREX I evaluation, was conducted in cooperation with the iris recognition industry to develop and test standard image formats, and to demonstrate that iris recognition algorithms can maintain their accuracy and interoperability with compact images. Standard formats are needed in federated applications in which iris data is exchanged between interoperating systems. Compact size is a current and vital requirement for applications in which imagery is passed across bandwidth-limited networks, or stored on identity credentials.

MARK YOUR CALENDAR

Federal Information Systems Security Educator's Association (FISSEA) Annual Conference

Dates: March 23-25, 2010

Place: National Institutes of Health, Natcher Conference Center, Bethesda, Maryland

Sponsors: NIST and FISSEA

The theme for FISSEA 2010 is "*Unraveling the Enigma of Role-Based Training.*" The first two days of the three-day conference will include one track devoted to role-based training and a second track focusing on awareness, training, education, and certification topics. The third day will feature a special emphasis on Cyber Security Initiatives. Captain Cheryl Seaman is the Conference Director and Daniel Benjamin is the Program Director.

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

Conference Web site: <http://csrc.nist.gov/fissea>

9th Symposium on Identity and Trust on the Internet (IDtrust 2010)

Dates: April 13-15, 2010

Place: NIST, Gaithersburg, Maryland

Sponsors: NIST, Internet2, Organization for the Advancement of Structured Information Standards (OASIS) IDtrust Member Section and Federal Public Key Infrastructure Policy Authority (FPKIPA)

With a conference theme of secure and convenient access control, IDtrust is looking for papers related to all parts of the public-key mediated authentication and access control problem. All software systems, from enterprise data centers to small businesses and consumer-facing applications, must make access control decisions for protected data. IDtrust is a venue for the discussion of the complete access control process (authentication, authorization, provisioning and security decision workflow), addressing questions such as: "What are the authorization strategies that will succeed in the next decade?" "What technologies exist to address complex requirements today?" "What research is academia and industry pursuing to solve the problems likely to show up in the next few years?"

Note: Identity as used here refers to not just the principal identifier, but also to attributes and claims.

NIST contact: Tim Polk, 301/975-3348, william.polk@nist.gov

Conference Web site: <http://middleware.internet2.edu/idtrust/>

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.