Information Technology Laboratory Newsletter

INSIDE THIS ISSUE

From left: Yee-Yin Choong, Ross Micheals, Mary Frances Theofanos, and Brian Stanton (Matthew Aronoff not pictured) received the Department of Commerce Bronze Medal Award for their work with handheld mobile biometrics devices. Credit: Denease Anderson (NIST)

January—February 2013

Issue 121

ITL Research Improves the Usability of Mobile Biometric Systems

The FBI's Hostage Rescue Team (HRT) presented NIST with a challenge: to design fingerprint capture software capable of running on a small hardware platform and having a touch interface. The interface had to be able to enter biographic information, control the fingerprint capture device, and display the resulting prints, all on a screen the size of an index card. The system was to be used in high-stress situations by the HRT in fulfilling their anti-terrorism duties. These duties required a portable and intuitive system that could be transported, deployed, and operated quickly.

In response to this challenge, NIST's Mary Frances Theofanos, Matthew Aronoff (formerly of NIST), Yee-Yin Choong, Ross Micheals, and Brian Stanton conducted a number of requirements-gathering exercises. First they performed task analyses. These analyses consisted of documenting the HRT's actions as they performed biometric captures in a simulated environment. One-on-one interviews followed to document any individual requirements. Lastly, the researchers conducted a group brainstorming session to work out detailed operational requirements. The requirements-gathering effort resulted in high-fidelity prototypes and detailed operational use cases.

This work represents the first-of-its-kind design and demonstration of a mobile biometric system implemented on a smart phone and a successful user-centered design approach to meet user requirements. Based on this success, the FBI is adopting the user-centered design approach on other projects, and several government agencies are exploring the smart phone platform for mobile biometric applications. The work opened up a new era of handheld biometric devices for federal, state, and local law enforcement agencies. The research team was recognized for dramatically improving the usability of the biometrics acquisition user interface for handheld touch-screen mobile biometrics devices by receiving a 2012 Department of Commerce Bronze Medal Award. For more information, see the NIST Mobile ID website.

.

ITL’s Cryptographic Module Validation Program

The Cryptographic Module Validation Program (CMVP) recently achieved a significant milestone by issuing the program’s 1,850th validation certificate. The program validates cryptographic modules for conformance to Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*. A joint program between NIST/ITL and the Computer Security Establishment Canada (CSEC) launched in 1995, the CMVP performs research and development to specify the test metrics and testing methods and develops implementation guidance utilized for laboratory conformance testing. Cryptographic modules are tested by independent, accredited laboratories in the United States, Canada, Germany, Spain, Japan, Taiwan, and Australia; twenty-one laboratories have been accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) to date. All completed laboratory test reports are reviewed by the CMVP to ensure laboratory competence, consistency, and completeness of the performed testing prior to a module’s validation as meeting security requirements at one of four levels. ITL’s Computer Security Division and the CSEC serve as validation authorities for the program. For more information, see the CMVP website.

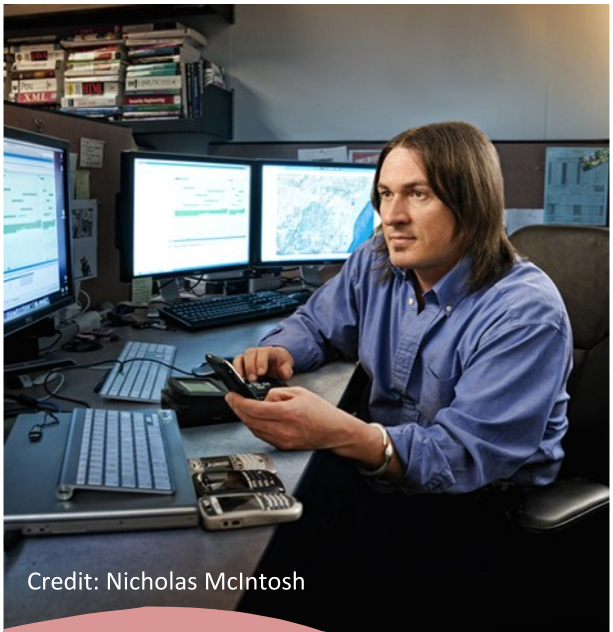
The CMVP Validated Modules List has become a “Who’s Who” of cryptographic and information technology vendors and developers from the United States, Canada, and worldwide. The list contains a complete range of security levels and a broad spectrum of module types such as secure radios, Internet browsers, digital projectors, disk/file encryptors, Smart Phones, Smart Cards, Virtual Private Network (VPN) devices, postage equipment, hardware accelerators, secure tokens, Satellite Communications, Department of Defense applications, and software toolkits, to name a few. The 1,850 certificates actually represent almost 4,250 separate modules by over 400 different vendors worldwide.

2012 ITL STAFF RECOGNITION

Jeremy Grant, head of the National Strategy for Trusted Identities in Cyberspace (NSTIC) National Program Office, and **Dawn Leaf**, former senior advisor for cloud computing at NIST, were selected by *FierceGovernmentIT* for the first annual “Fierce 15” list of top federal employees. The award recognizes work on current progressive projects in government, honoring those who work tirelessly to make government more efficient, service- and mission-oriented, and accountable.

Kevin Stine, group manager in the Computer Security Division, was recently designated by the Workgroup for Electronic Data Interchange (WEDI) Board of Directors as a recipient of the 2012 WEDI Award of Merit. WEDI brings together a consortium of leaders within the healthcare industry to identify practical strategies for reducing administrative costs in healthcare through the implementation of electronic data interchange. The award recognizes individuals who have contributed in a meaningful way to the success of WEDI programs through their volunteer commitment and talents.

Ya-Shian Li-Baboud, computer scientist in the Software and Systems Division, received the Department of Commerce Bronze Medal for her efforts that paved the way for industrial advances in improving the dynamic situational awareness and intelligence of the Smart Grid.



Credit: Nicholas McIntosh

Richard P. Ayers, computer scientist in the Software and Systems Division, received the Department of Commerce Bronze Medal for developing mobile device forensic formal specifications and test methods needed for successful investigation and prosecution of crimes involving mobile devices.

Selected New Publications

The Twentieth Text REtrieval Conference Proceedings (TREC 2011)
Ellen M. Voorhees and Lori P. Buckland, Editors
NIST Special Publication 500-296
October 2012

This report constitutes the proceedings of the Twentieth Text REtrieval Conference (TREC 2011) held at NIST on November 15-18, 2011. The conference was cosponsored by NIST, the Defense Advanced Research Projects Agency (DARPA), and the Advanced Research and Development Activity (ARDA).

Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
By Morris Dworkin
NIST Special Publication 800-38F
December 2012

This publication describes cryptographic methods that are approved for "key wrapping," i.e., the protection of the confidentiality and integrity of cryptographic keys. In addition to describing existing methods, the publication specifies two new deterministic authenticated-encryption modes of operation of the Advanced Encryption Standard (AES) algorithm: the AES Key Wrap (KW) mode and the AES Key Wrap with Padding (KWP) mode. An analogous mode with the Triple Data Encryption Algorithm (TDEA) as the underlying block cipher, called TKW, is also specified, to support legacy applications.

Recommendation for Cryptographic Key Generation
By Elaine Barker and Allen Roginsky
NIST Special Publication 800-133
December 2012

Cryptography is often used in an information technology security environment to protect data that is sensitive, has a high value, or is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage. Cryptography relies upon two basic components: an algorithm (or cryptographic methodology) and a cryptographic key. This Recommendation discusses the generation of the keys to be managed and used by the approved cryptographic algorithms.

A Credential Reliability and Revocation Model for Federated Identities
By Hildegard Ferraiolo
NISTIR 7817
November 2012

A large number of Identity Management Systems (IDMSs) are being deployed worldwide that use different technologies for the population of their users. With the diverse set of technologies, and the unique business requirements for organizations to federate, there is no uniform approach to the federation process. Similarly, there is no uniform method to revoke credentials or their associated attribute(s) in a federated community. In the absence of a uniform revocation method, this document seeks to investigate credential and attribute revocation with a particular focus on identifying missing requirements. The document introduces and analyzes the different types of digital credentials and recommends missing revocation-related requirements for each model in a federated environment. The paper also suggests a credential reliability and revocation service that serves to eliminate the missing requirements.

Combinatorial Coverage Measurement
By D. Richard Kuhn, Raghu N. Kacker, and Yu Lei
NISTIR 7878
October 2012

Combinatorial testing applies factor covering arrays to test all t-way combinations of input or configuration state space. In some testing situations, it is not practical to use covering arrays, but any set of tests with n parameters covers at least some proportion of t-way combinations up to t ≤ n. This report describes measures of combinatorial coverage that can be used in evaluating the degree of t-way coverage of any test suite, regardless of whether it was initially constructed for combinatorial coverage.

Statistical Analysis of Reader Management Variability in Nodule Sizing with CT Phantom Imaging Data
By Zhan-Qian John Lu, Charles Fenimore, Nicholas Petrick, Rongping Zeng, Marios A. Gavrielides, David
Clunie, Kristin Borradaile, Robert Ford, Hyun J. Grace Kim, Michael F. McNitt-Gray, Binsheng Zhao, and Andrew J. Buckler
NISTIR 7879
November 2012

A study was performed under the auspices of Radiological Society of North America (RSNA) as a component of the Quantitative Imaging Biomarker Alliance (QIBA) to assess reader measurement variability of both spherical and complex (non-spherical) nodules sizing measures based on CT imaging scans. This paper reports the statistical data analysis of intra-reader and inter-reader variability of the three sizing measurements (1D, 2D, and 3D) performed as part of this collaborative effort. An analysis of variance strategy is presented to analyze a well-designed experiment with complex factor settings and reader variability is defined.

Significant Test in Speaker Recognition Data Analysis with Data Dependency
By Jin Chu Wu, Alvin F. Martin, Craig S. Greenberg, Raghu N. Kacker, and Vincent M. Stanford
NISTIR 7884
October 2012

To evaluate the performance of speaker recognition systems, a detection cost function defined as a weighted sum of the probabilities of type I and type II errors is employed. The speaker datasets may have data dependency due to multiple uses of the same subjects. Using the standard errors of the detection cost function computed by means of the two-layer nonparametric two-sample bootstrap method, a significance test is performed to determine whether the difference between the measured performance levels of two speaker recognition algorithms is statistically significant. While conducting the significance test, the correlation coefficient between two detection cost functions for two algorithms, respectively, is taken into account. Examples are provided.

Upcoming Technical Conferences

NIST Joint Cloud and Big Data Workshop

Dates: January 15-17, 2013
Place: NIST, Gaithersburg, MD
Cost: None

The workshop will bring together leaders and innovators from industry, academia and government in an interactive format that combines keynote presentations, panel discussions, interactive breakout sessions, and open discussion. The conference will be led off by Pat Gallagher, Under Secretary of Commerce for Standards and Technology and Director, NIST, and Steven VanRoekel, the Chief Information Officer of the United States. The workshop will explore possibilities for harmonizing Cloud and Big Data measurement, benchmarking, and standards in ways that bring the power of these two approaches to bear in driving progress and prosperity.
NIST contact: Robert Bohn, robert.bohn@nist.gov

ANSI/NIST-ITL Standard Workshop 2013

Dates: January 28-30, 2013
Place: NIST, Gaithersburg, Maryland
Cost: None

The workshop will provide an opportunity to review current developments on the Dental and Oral Forensics Supplement to the standard; the Forensic and Investigatory Voice Supplement to the standard; best practices for data transfer concerning Unknown Deceased and Living Amnesiacs; a new approach to mobile biometric data transmission "ANSI/NIST-ITL LITE"; and a concept of having a standard for data transmission concerning object identification, such as cartridges, bullets, tire tracks, shoe prints, and inks.
NIST contact: Brad Wing, bradford.wing@nist.gov

Future of Voting Systems Symposium

Dates: February 26-28, 2013
Place: NIST, Gaithersburg, Maryland
Sponsors: NIST and the U.S. Election Assistance Commission
Cost: $270

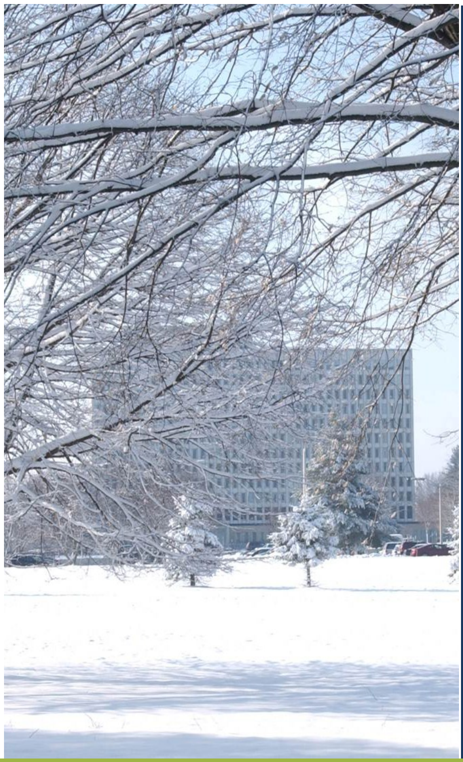
This symposium will explore emerging trends in voting system technology with the diverse election community at large. Topics include trends in voting system technology acquisition and deployment plans; how election officials, manufactures, young voters, and academics view the future of voting system technologies; and alternative standard development processes for voting systems.
NIST contact: Mary Brady, mary.brady@nist.gov

26th Annual Federal Information System Security Education Association (FISSEA) Conference

Dates: March 19-21, 2013
Place: NIST, Gaithersburg, Maryland
Audience: Government/Industry/Academia
Sponsors: NIST and FISSEA
Cost: TBD

Founded in 1987, FISSEA is an organization run by and for federal information systems security professionals. FISSEA assists federal agencies in meeting their computer security training responsibilities. The theme of their 2013 conference is “Making Connections in Cybersecurity and Information Security Education.”
NIST contacts: Patricia Toth, patricia.toth@nist.gov, and Peggy Himes, peggy.himes@nist.

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 at 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