

ITL NEWSLETTER FOR FEBRUARY 2009

ITL ADVANCES THE STATE OF THE ART IN TEXT RETRIEVAL AND ANALYSIS

The Information Access Division, in collaboration with ITL's Information Discovery, Use and Sharing Program, recently hosted the seventeenth annual Text REtrieval Conference (TREC). TREC serves the information retrieval research community by providing the infrastructure for large-scale evaluation of search technologies. Co-located with TREC this year was the inaugural Text Analysis Conference (TAC). TAC extends the benefits of community-wide evaluation to natural language processing tasks. Both the TREC and TAC workshops included presentations of results for each of the 2008 tracks (including failure analyses and system comparisons), as well as more lengthy system presentations describing techniques used, experiments run on the data, and other issues of interest to the researchers.

To foster collaboration among the communities served by TREC and TAC, ITL defined a series of interrelated tasks that spanned the two conferences. In the TREC blog track, participants developed systems that detect opinionated posts regarding a given target from a large collection of blog posts. Participants in the TAC question answering track developed systems that recognize the snippets within the posts that are expressions of the opinions, while TAC summarization systems constructed concise, coherent summaries of the opinions regarding the target from the snippets.

A second TREC track focused on defining efficient, effective procedures for legal discovery of electronically stored information during litigation and regulatory actions. Now in its third year, TREC's legal discovery track has been cited in a judicial decision as a cause for optimism that new methods will soon be found which will reduce the costs associated with legal discovery.

TREC and TAC 2008 each attracted more than 50 participating groups from industry, academia, and government. The conferences had strong international support with more than 20 countries represented spanning six continents. More details are available at <http://trec.nist.gov> and <http://www.nist.gov/tac>.

ITL Demonstrates Successful Testing Strategy at Health IT Event

Approximately 80 participants from 23 private and public organizations recently convened at NIST for a Nationwide Health Information Network (NHIN) test event. NHIN is a Department of Health and Human Services (HHS) initiative to use voluntary consensus-based standards to exchange clinical health information among doctors, consumers, and other healthcare professionals. ITL has the lead role in defining the testing strategy for the NHIN.

The participating private industry organizations generally serve to help exchange clinical information within a given region. For example, the organization from Indiana provides a service to many hospitals, clinicians, laboratories, etc., that helps them share clinical information with each other. These organizations are either under contract to HHS or are a grantee to HHS to participate in this project. Most of the large providers of healthcare services in the federal government also participated in the event, including the Centers for Disease Control, the Department of Defense, the Indian Health Service, the Social Security Administration, and the Department of Veterans Affairs.

The goals of the testing event were to determine if NHIN participants have correctly implemented NHIN specifications and can exchange clinical healthcare information with each other; to determine if NHIN specifications are helpful in achieving the information exchange goals of the NHIN; and to provide any feedback to standards development organizations with respect to any ambiguities or inconsistencies uncovered during the testing process. The results of the event facilitated a public forum demonstrating the interoperability of the participants in the NHIN Trial Implementations in Washington, D.C. The website is <http://xreg2.nist.gov/hit-testing/>.

UPDATE ON NEW PUBLICATIONS

See ITL's new brochure detailing our mission, programs, and resources at http://www.itl.nist.gov/ITLBrochure_010509.pdf.

Security Considerations in the System Development Life Cycle

By Richard Kissel, Kevin Stine, Matthew Scholl, Hart Rossman, Jim Fahlsing, and Jessica Gulick

NIST Special Publication 800-64, Rev. 2

October 2008

<http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf>

This publication assists federal agencies in integrating essential information technology (IT) security steps into their established IT system development life cycle (SDLC). This process should result in more cost-effective, risk-appropriate security control identification, development, and testing.

An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

By Matthew Scholl, Kevin Stine, Joan Hash, Pauline Bowen, Arnold Johnson, Carla Dancy Smith, and Daniel I. Steinberg

NIST Special Publication 800-66, Rev. 1

October 2008

<http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf>

This document discusses security considerations and resources that may provide value when implementing the requirements of the HIPAA Security Rule. It defines information security terms and standards used in the rule and directs readers to helpful information in other NIST publications on individual topics addressed by the HIPAA Security Rule. The publication does not supplement, replace, or supersede the HIPAA Security Rule itself.

Guide to Securing Microsoft Windows XP Systems for IT Professionals

By Murugiah Souppaya and Karen Scarfone

NIST Special Publication 800-68, Rev. 1

October 2008

http://csrc.nist.gov/itsec/download_WinXP.html

This publication assists IT professionals in securing Windows XP workstations, mobile computers, and computers used by telecommuters within various environments. The recommendations apply to Windows XP Professional systems running Service Pack 2 or 3. The publication recommends and explains tested, secure settings with the objective of simplifying the administrative burden of improving the security of Windows XP systems in five types of environments: small office/home office, enterprise, specialized security-limited functionality, legacy, and Federal Desktop Core Configuration (FDCC).

Recommendation for Key Derivation Using Pseudorandom Functions

By Lily Chen

NIST Special Publication 800-108

November 2008

<http://csrc.nist.gov/publications/nistpubs/800-108/sp800-108.pdf>

This recommendation specifies techniques for the derivation of additional keying material from a secret key, either established through a key establishment scheme or shared through some other manner, using pseudorandom functions.

A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)

By William MacGregor, Ketan Mehta, David Cooper, and Karen Scarfone

NIST Special Publication 800-116

November 2008

<http://csrc.nist.gov/publications/nistpubs/800-116/SP800-116.pdf>

This document provides best-practice guidelines for integrating the PIV Card with the physical access control systems (PACS) that authenticate the cardholders in federal facilities. Specifically, the document recommends a risk-based approach for selecting appropriate PIV authentication mechanisms to manage physical access to federal government facilities and assets. The document also proposes a PIV implementation maturity model to measure the progress of facility and agency implementations.

Guidelines on Cell Phone and PDA Security

By Wayne Jansen and Karen Scarfone

NIST Special Publication 800-124

October 2008

<http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf>

This document provides an overview of cell phone and PDA devices in use today and offers insights into making informed information technology security decisions on their treatment. The document gives details about the threats and technology risks associated with these devices and the available safeguards to mitigate them. Organizations can use this information to enhance security and reduce incidents involving handheld devices.

Symmetric Key Injection onto Smart Cards

By David Cooper and William MacGregor

NISTIR 7539

December 2008

<http://csrc.nist.gov/publications/PubsNISTIRs.html>

This paper describes architectures for securely injecting secret keys onto smart cards. Specifically, the paper details key injection architectures based on the identity credentials available on the Personal Identity Verification (PIV) Card. The primary goal is to create additional opportunities for the use of the PIV Card in Physical Access Control Systems (PACS). The paper identifies ways to load site-specific symmetric keys onto a PIV Card after the card has been issued, which allows each smart card to share a unique secret key with each PACS with which it interacts.

Assessing Face Acquisition

By Mary Theofanos, Brian Stanton, Charles Sheppard, Ross Micheals, J. Libert, and S. Orandi

NISTIR 7540

November 2008

http://zing.ncsl.nist.gov/biousa/docs/face_IR-7540.pdf

This paper discusses the usability components of the face image capture process that contribute to the relatively high ratio of unusable images collected by U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT). It introduces a general evaluation methodology—including the use of a simple image overlay—to quantify various characteristics of face imagery. The experimental context mimicked the point-of-entry environment, but with specific usability enhancements. The collected data suggests that these usability enhancements may improve face image capture with equipment that is capable of capturing faces with a near-zero failure-to-enroll (FTE) rate.

The Last 1% - Biometric Quality Assessment for Error Suppression

By Elham Tabassi and Patrick Grother

NISTIR 7544

November 2008

elham.tabassi@nist.gov

Biometric quality measurement algorithms are increasingly deployed in operational systems; US-VISIT, PIV, and EU VIS each mandate the measurement and reporting of quality scores of captured images. With the increase in deployment of quality algorithms, the need to standardize an interoperable way to store and exchange biometric quality scores, and methods for evaluation the effectiveness of quality algorithms increases. This document describes NIST's activities on biometric sample quality research and standardization.

A Threat Analysis on UOCAVA Voting Systems

By Andrew Regenscheid and Nelson Hastings

NISTIR 7551

December 2008

<http://vote.nist.gov/uocava-threatanalysis-final.pdf>

This report presents the results of ITL's research into technologies to improve the voting process for U.S. citizens living overseas. It splits the overseas voting process into three stages: voter registration and ballot request, blank ballot delivery, and voted ballot return. For each stage, the report describes how various transmission options could be used to support overseas voting. The transmission options discussed are postal mail, telephone, fax, electronic mail, and web-based systems. As part of the analysis, mitigating controls for each threat are provided when possible; these provide the basis for an effort to develop best practices for overseas voting systems.

MARK YOUR CALENDAR

First SHA-3 Candidate Conference

Dates: February 25-27, 2009 (in conjunction with the Fast Software Encryption Workshop)

Location: Leuven, Belgium

NIST is conducting a public competition to develop a new cryptographic hash algorithm, which converts a variable length message into a short "message digest" that can be used for digital signatures, message authentication, and other applications. The competition is NIST's response to recent advances in the cryptanalysis of hash algorithms. The new hash algorithm will be called "SHA-3" and will augment the hash algorithms currently specified in FIPS 180-2, *Secure Hash Standard*. The deadline for entries for the competition was October 31, 2008. NIST is reviewing the submitted algorithms and selecting candidates that meet the basic submission requirements.

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

Conference website: <http://www.nist.gov/hash-competition/>

22nd Annual Federal Information Systems Security Educators' Association (FISSEA) Conference

Dates: March 24-26, 2009

Place: NIST, Gaithersburg, Maryland

Sponsors: FISSEA, NIST

This year's conference theme is "Awareness, Training, and Education – The Catalyst for Organizational Change." Presentation topics include awareness programs, training methods, educational activities, compliance regulations, professional certification, organizational impacts of these programs, the management of information security programs and personnel, supporting technologies, and emerging trends.

NIST contact: Mark Wilson, 301/975-3870, mark.wilson@nist.gov

Conference website: <http://csrc.nist.gov/organizations/fissea/2009-conference/index.shtml>

8th Symposium on Identity and Trust on the Internet (IDtrust 2009)

Dates: April 14-16, 2009

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)

The conference theme is “Authorization and Attributes.” IDtrust is devoted to research and deployment experience related to making good security decisions based on identity information, especially when public key cryptography is used and the human elements of usability are considered. The success of any business strategy depends on having the right people gain access to the right information at the right time. This implies that an IT infrastructure has - among other things - an authorization framework in place that can respond to dynamic security conditions and regulatory requirements quickly, flexibly, and securely. 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?

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

Conference website: <http://middleware.internet2.edu/idtrust/>

Elizabeth B. Lennon, Editor
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

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.