Information Technology Laboratory Newsletter

Credit: NIST

March—April 2014

Issue 128

INSIDE THIS ISSUE

NIST Releases Cybersecurity Framework for Critical Infrastructure

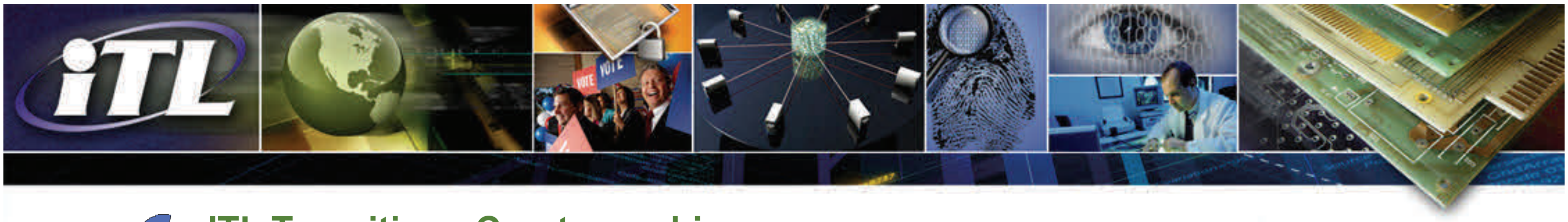
On February 13, 2014, NIST released the Framework for Improving Critical Infrastructure Cybersecurity Version 1.0. Created through a government, industry, and academia partnership, the Framework consists of standards, guidelines, and best practices to strengthen the cybersecurity of our nation's critical infrastructure. The Framework uses a flexible and cost-effective approach to help owners and operators of critical infrastructure to reduce and manage their cyber risks.

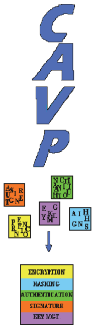
The Framework is risk-based and consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. It seeks to promote the wide adoption of practices to increase cybersecurity across all sectors and industry types. The Framework provides a common taxonomy and mechanism, based on existing standards, guidelines, and practices, for organizations to:

- Describe their current cybersecurity posture;
- Describe their target state for cybersecurity;
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
- Assess progress toward the target state; and
- Communicate among internal and external stakeholders about cybersecurity risk.

NIST developed the framework in response to Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, which President Obama issued in February 2013. The Executive Order stated: "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats." The directive tasked NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cybersecurity risks. Led by ITL, the Framework was developed by ongoing engagement with, and input from, stakeholders in government, industry, and academia over the past year. The open public review and comment process started with a Request for Information in the Federal Register dated February 26, 2013, and included a series of five public workshops held at various locations throughout the United States.

NIST also released a companion Roadmap document that details the agency's next steps with the Framework. The Roadmap identifies key areas of future cybersecurity development and collaboration. As the Framework and Roadmap are "living" documents, we welcome your ongoing suggestions and feedback at cyberframework@nist.gov.





ITL Transitions Cryptographic Algorithms and Key Lengths to Stronger Cryptographic Keys

Effective January 1, 2014, key lengths providing less than 112 bits of security strength are no longer approved to generate digital signatures, as recommended in NIST Special Publication (SP) 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*. In addition, the use of Secure Hash Algorithm (SHA)-1 with Digital Signature Generation is no longer approved. ITL's Computer Security Division published SP 800-131A in January 2011 to prepare for the transitioning of cryptographic algorithms and key lengths to stronger cryptographic keys and more robust algorithms.

The Cryptographic Algorithm Validation Program (CAVP) and the Cryptographic Module Validation Program (CMVP) issued Implementation Guidance (IG) G.14, Validation of Transitioning Cryptographic Algorithms and Key Lengths, to discuss how the validation of the cryptographic algorithms and cryptographic modules will be affected during the transition as specified in SP 800-131A. The highlights of the transition include the removal of the modulus and curve sizes that provide less than 112 bits of security strength from the Signature Generation function of the affected cryptographic algorithm validation lists, since they are now non-approved elements of the algorithm. These include the 1024-bit modulus size for DSA, modulus sizes of 1024 and 1536 bits for RSA, and the P-192, K-163 and B-163 curves for ECDSA. In addition, the SHA-1 hash algorithm has been removed for every remaining allowed modulus size used for signature generation. The CAVP has created a historical algorithm validation list for every cryptographic algorithm affected by this transition to maintain a record of the disallowed features. See CMVP IG G.14 for more details.

Credit: Shutterstock

Also, effective January 1, 2014, the CAVP and the CMVP will not be validating new implementations of Federal Information Processing Standard (FIPS) 186-2, Key Pair Generation and Signature Generation. The CMVP issued IG G.15, Validating the Transition from FIPS 186-2 to FIPS 186-4, in January 2011 to assist users in the transition from FIPS 186-2 to FIPS 186-4. See CMVP IG G.15 for more details.

Refer to the http://csrc.nist.gov/groups/STM/cavp/ and http://csrc.nist.gov/groups/STM/cmvp/ websites for more information on the CAVP and CMVP, the FIPS-approved and NIST-recommended cryptographic algorithms currently validated by the CAVP, and the historical validation lists containing records of the disallowed features of previously validated algorithmic implementations. The CAVP and the CMVP are collaborative programs between NIST and the Communication Security Establishment of the Canadian Government (CSEC).

ITL's Text REtrieval Conference Supports the Information Retrieval Research Community

ITL recently sponsored the 22nd Text REtrieval Conference (TREC) at the NIST Gaithersburg campus. ITL founded and directs the international TREC project, an effort that develops the infrastructure required to measure the effectiveness of information retrieval systems, e.g., search engines.

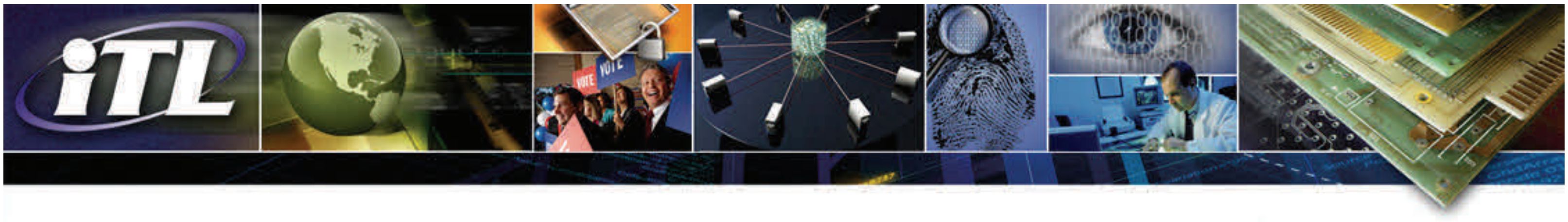
Each TREC is organized around a set of focus areas called tracks. TREC participants use their own search engines and a common data set to perform a track's task. They submit their results to ITL researchers, who use the combined result sets to build evaluation resources that are then used to score each participant's submission. These resources are eventually made publicly available through the TREC website to support the larger retrieval research community.

TREC 2013 contained eight tracks and received search result submissions from 60 research groups in 21 countries. The 2013 tracks investigated several topics including best practices in crowdsourcing for the development of search evaluation resources, the real-time nature of search in "microblogs" (e.g., Twitter tweets), and diversifying result sets in web search. Two of the tracks were new to TREC 2013. The Federated Web Search track investigates techniques for metasearching: selecting which sites to search and combining result sets to form a single coherent response from among a large set of independent search verticals. The Temporal Summarization track looks to develop systems that allow users to efficiently monitor the information associated with an event such as a natural disaster in real time. Proceedings of TREC 2013 will be posted on the TREC website .

Staff Recognition

Jonathon Phillips, Information Access Division, received the inaugural Mark Everingham Prize from the Institute of Electrical and Electronics Engineers (IEEE) Pattern Analysis and Machine Intelligence (PAMI) Technical Committee. The prize recognized Phillips for his work on a series of datasets and challenges starting with the Face Recognition Technology (FERET) evaluations in the 1990s, the Face Recognition Grand Challenge in 2004-2005, and Face Recognition Vendor Tests in 2000, 2002, and 2006. These efforts were significant because they established the challenge paradigm as a key method to facilitate the development of new and improved algorithms in the computer vision and pattern recognition community.

Credit: NIST



Selected New Publications

Compression Guidance for 1000 ppi Friction Ridge Imagery

By Shahram Orandi, John Libert, John Grantham, Kenneth Ko, Stephen Wood, Frederick Byers, Bruce Bandini, Stephen Harvey, and Michael Garris
NIST Special Publication 500-289
February 2014

The criminal justice community has traditionally captured, processed, stored, and exchanged friction ridge imagery data at 500 ppi in the course of their operation. Modern biometric systems are trending towards operation on fingerprint images at 1000 ppi. This transition to 1000 ppi friction ridge imagery offers many benefits, notably greater fidelity to the original sample and better representation of Level 3 features. Both of these benefits are favorable since they may increase probability of establishing a match/non-match decision by expert examiners or automated fingerprint matchers. The JPEG2000 compression standard offers much flexibility in the types of images it can operate on as well as the way images can be compressed and encoded. This flexibility makes it a suitable compression algorithm for friction ridge imagery. A need exists for a normative guidance that establishes a set of protocols for the compression of images by stakeholders. Adherence to this normative guidance by stakeholders provides assurances for compatibility between those stakeholders. This publication provides normative guidance for compression of grayscale friction ridge imagery at 1000 ppi.

Security and Privacy Controls for Federal Information Systems and Organizations

Joint Task Force Transformation Initiative
NIST Special Publication 800-53 Revision 4 Errata
January 2014

Including updates as of January 15, 2014, this publication provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations, organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors. The controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk. The controls address a diverse set of security and privacy requirements across the federal government and critical infrastructure, derived from legislation, Executive Orders, policies, directives, regulations, standards, and/or mission/business needs. Addressing both security functionality and security assurance ensures that information technology products and the information systems built from those products using sound systems and security engineering principles are sufficiently trustworthy.

Guide to Attribute-Based Access Control (ABAC) Definition and Considerations

By Vincent Hu, David Ferraiolo, Rick Kuhn, Adam Schnitzer, Kenneth Sandlin, Robert Miller, and Karen Scarfone
NIST Special Publication 800-162
January 2014

This document provides federal agencies with a definition of attribute-based access control (ABAC). ABAC is a logical access control methodology where authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes. The document also provides considerations for using ABAC to improve information sharing within organizations and between organizations while maintaining control of that information.

Estimation of Uncertainty in Application Profiles

By David W. Flater
NIST Technical Note 1826
January 2014

Application profiling tools are the instruments used to measure software performance at the function and application levels. The most powerful measurement method available in application profiling tools today is sampling-based profiling, where a potentially unmodified application is interrupted based on some event to collect data on what it was doing when the interrupt occurred. It is well known that sampling introduces statistical uncertainty that must be taken into account when interpreting results; however, factors affecting the variability have not been well-studied. In attempting to validate two previously published analytical estimates, we obtained negative results. Furthermore, we found that the variability is strongly influenced by at least one factor, self-time fragmentation, which cannot be determined from the data yielded by sampling alone. We investigate this and other factors and conclude with recommendations for obtaining valid estimates of uncertainty under the conditions that exist.

A Spectral Analytic Method for Fingerprint, Image Sample Rate Estimates

By John M. Libert, Shahram Orandi, John Grantham, and Michael Garris
NISTIR 7968
March 2014

This study examines the use of the NIST Spectral Image Validation and Verification (SIVV) metric for the application of detecting the sample rate of a given fingerprint digital image. SIVV operates by reducing an input image to a 1-dimensional power spectrum that makes explicit the characteristic ridge structure of the fingerprint that on a global basis differentiates it from most other images. The magnitude of the distinctive spectral feature, which is related directly to the distinctness of the level 1 ridge detail, provides a primary diagnostic indicator of the presence of a fingerprint image. The location of the detected peak corresponding to the level 1 ridge detail can be used as an estimator of the original sampling frequency of that image given the behavior of this peak at known sampling frequencies a priori versus the calculated shift of this peak on an image of unknown sampling rate. A statistical model is fit to frequency measurements of a sample of images scanned at various sample rates from 10-print fingerprint cards such that the model parameters can be applied to SIVV frequency values of a digital fingerprint of unknown sample rate to estimate the sample rate. Uncertainty analysis is used to compute 95 % confidence intervals for predictions of sample rate from frequency. The model is tested against sets of cardscan and livescan images.

Upcoming Technical Conferences

Static Analysis Tool Exposition (SATE) V Experience Workshop
Date: March 14, 2014
Place: NIST, Gaithersburg, Maryland
Cost: None

Software must be developed to have high quality; quality cannot be “tested in.” For maximum reliability and assurance, static analysis must be used in addition to good development and testing. This workshop will bring together researchers, tool developers, and users of software assurance tools to share experiences, report observations, define obstacles, and identify engineering or research approaches to overcome obstacles to software assurance capabilities.
NIST contact: Elizabeth Fong

FISSEA Annual Conference
Dates: March 18-20, 2014
Place: NIST, Gaithersburg, Maryland
Sponsors: NIST and FISSEA
Cost: $184

The theme of this year’s Federal Information Systems Security Educators’ Association (FISSEA) conference will be “Partners in Performance: Shaping the future of cybersecurity Awareness, Education and Training.” Presentations will reflect current projects, trends, and initiatives that provide for future solutions in security programs. NIST contact: Peggy Himes

Cloud Computing Forensic Science Workshop
Date: March 24, 2014
Place: NIST, Gaithersburg, Maryland
Cost: None

This workshop will present experts in the fields of cloud, digital forensics, and measurement for sessions on the perspectives, vision, current state, and future of cloud forensic science. Leaders in cloud computing and digital forensics from government, industry, and academia should attend, as well as architects, researchers, and implementers of cloud computing and digital forensics technologies. NIST contact: Michaela Iorga,

The Intersection of Cloud and Mobility
Dates: March 25-27, 2014
Place: NIST, Gaithersburg, Maryland
Cost: None
As part of its continuing cloud computing series, ITL is sponsoring a new forum on cloud and mobility. Topics will include federal perspectives on and vision of cloud and mobility, current and future intersections of cloud and mobility, challenges and lessons learned, and the path forward to a federated mobile cloud.
NIST contacts: Michaela Iorga and Frederic de Vaulx

Privacy Engineering Workshop
Dates: April 9-10, 2014
Place: NIST, Gaithersburg, Maryland
Cost: None

The workshop will focus 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. By examining existing models such as security engineering and safety risk management, the workshop will explore the concepts of a privacy risk management model, privacy requirements and system design and development.
NIST contact: Suzanne Lightman

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 in 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