FY 2005 ITL Publications

Note that some documents are published in more than one place. Due to the large number of documents, publications listed in prior-year publication lists are not repeated.

Anderson, D.M., Cermeli, P., Fried, E., Gurtin, M.E., McFadden, G.B., *General Dynamical Sharp-interface Conditions for Phase Transformations in Viscous Heat-Conducting Fluids*, Journal of Fluid Mechanics, to be published

The purpose of this paper is to develop, from basic considerations, a complete set of equations governing the evolution of a sharp interface separating two fluid phases undergoing transformation. For situations in which a phase transformation does not occur, so that the phase interface is a material surface, the governing bulk and interfacial equations are well-developed and agreed upon. Focusing on the interface, the relevant equations are the conventional balances for mass, linear momentum, and energy, augmented by suitable constitutive equations. But when a phase transformation does occur, the interfacial expressions for balance of mass, momentum, and energy fail to provide a closed description and must be supplemented by an equation that accounts for the microphysics underlying the exchange of material between phases. For this purpose we employ the formalism of configurational forces to derive the appropriate generalization of the Gibbs-Thomson equation for a fluid-fluid interface under non-equilibrium conditions.

Arlandis, J., Over, P., Kraaij, W., *Boundary Error Analysis and Categorization in the TRECVID News Story Segmentation Task*, Conference on Image and Video Retrieval

In this paper, an error analysis based on boundary error popularity including semantic boundary categorization is applied in the context of the news story segmentation task from TRECVID, Clusters of systems were defined based on the input resources they used including video, audio and automatic speech recognition. A cross-popularity specific index was used to measure boundary error popularity across cluster, which allowed goal-driven selection of boundaries to be categorized. A wide set of boundaries was viewed and a summary of the error types is presented. This framework allowed drawing conclusions about the behavior of resource-based clusters in the context of news story segmentation.

Avilés, A.I., Ankenman, B.E., Pinheiro, J.C., *Assembled Designs for Estimation of Location, Dispersion, and Random Effects*, Technometrics, to be published

In many experimental settings, different types of factors affect the measured response. The factors that can be set independently of each other are called crossed factors. Nested factors cannot be set independently because the level of one factor takes on a different meaning when other factors are changed. Random nested factors arise from quantity designations and from sampling and measurement procedures. The variances of the random effects associated with nested factors are called variance components. Factor effects on the average are called location effects. Dispersion effects are the effects of the crossed factors on the variance of a response. For situations where crossed factors have effects on the different variance components, then sets of dispersion effects must be identified and estimated to achieve robustness. The main objective of this research is to provide nearly D-optimal experimental design procedures for estimating the location effects of crossed factors, the variance components associated with two nested factors, and the dispersion effects that crossed factors may have on the two variance components. A general class of experimental designs for mixed-effects models with random nested factors, called assembled designs, is introduced in Ankenman, Avilés, and Pinheiro (2003). The use of assembled designs for robustness experiments is introduced. When there are dispersion effects, a heuristic algorithm for finding a nearly D-optimal assembled design with two variance components for a given budget is provided. Ready to use computer programs for the presented experimental design procedures and analysis technique are discussed. This research provides the practitioner with clear guidelines about the best design available for their needs.

Ayers, R., Jansen, W., Cilleros, N., Daniellou, R., *Cell Phone Forensics Tools: An Overview and Analysis*, NISTIR 7250, to be published

Cell phones and other handheld devices incorporating cell phone capabilities (e.g., Personal Digital Assistants [PDAs] phones) are ubiquitous. Rather than just placing calls, certain phones allow users to perform additional tasks such as SMS (Short Message Service) messaging, Multi-Media Messaging Service (MMS) messaging, IM (Instant Messaging), electronic mail, Web browsing, and basic PIM (Personal Information Management) applications (e.g., phone and date book). PDA phones, often referred to as smart phones, provide users with the combined capabilities of both a cell phone and a PDA. In addition to network services and basic PIM applications, one can manage more extensive appointment and contact information, review electronic documents, give a presentation, and performing other tasks.

All but the most basic phones provide individuals with some ability to load additional applications, store and process personal and sensitive information independently of a desktop or notebook computer, and optionally synchronize the results at some later time. As digital technology evolves, the capabilities of these devices continue to improve rapidly. When cell phones or other cellular devices are involved in a crime or other incident, forensic examiners require tools that allow the proper retrieval and speedy examination of information present on the device. This report gives an overview of current forensic software, designed for acquisition, examination, and reporting of data discovered on cellular handheld devices, and an understanding of their capabilities and limitations.

Ban, K., Gharavi, H., *Group-Based Ad-hoc Network for Multimedia Communications*, 16th Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications, PIMRC 2005, Berlin, Germany, September 11-14, 2005

This paper is concerned with evaluating ad-hoc networks for group-oriented tactical operations. For such operations, a cellular-based ad-hoc network architecture has been constructed for real-time multimedia communications. To assess the suitability of this network, its performance has been compared with conventional peer-to-peer ad-hoc network architectures under various test scenarios using IEEE 802.11 WLAN technology. We have shown that the cellular network, which operates in two modes: infrastructure for intracell and ad-hoc for intercell communications, is more suitable for group-based tactical missions.

Barker, E., Barker, W., Burr, W., Polk, W., Smid, M., *Recommendation for Key Management, Part 1: General*, NIST SP 800-57, http://csrc.nist.gov/publications/nistpubs/index.html, August 2005

This Recommendation provides cryptographic key management guidance. The proper management of cryptographic keys is essential to the effective use of cryptography for security. Users and developers are presented with many choices in their use of cryptographic mechanisms. Inappropriate choices may result in an illusion of security, but little or no real security for the protocol or application. Ultimately, the security of information protected by cryptography directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with keys, and the protection afforded the keys. Cryptography can be rendered ineffective by the use of weak products, inappropriate algorithm pairing, poor physical security, and the use of weak protocols.

This recommendation is written for several different audiences and is divided into three parts. Part 1 of the recommendation:

1. Defines the security services that may be provided and key types employed in using cryptographic mechanisms.
2. Provides background information regarding the cryptographic algorithms that use cryptographic keying material.
3. Classifies the different types of keys and other cryptographic information according to their functions, specifies the protection that each type of information requires and identifies methods for providing this protection.
4. Identifies the states in which a cryptographic key may exist during its lifetime.
5. Identifies the multitude of functions involved in key management.
6. Discusses a variety of key management issues related to the keying material, including key usage, cryptoperiod length, domain parameter validation, public key validation, accountability, audit, key management system survivability, and guidance for cryptographic algorithm and key size selection.

Barker, E., Barker, W., Burr, W., Polk, W., Smid, M., *Recommendation for Key Management, Part 2: Best Practices for Key Management Organization*, NIST SP 800-57, http://csrc.nist.gov/publications/nistpubs/index.html, August 2005

"Best Practices for Key Management Organization," Part 2 of the Recommendation for Key Management is intended primarily to address the needs of system owners and managers. It provides context, principles, and implementation guidelines to assist in implementation and management of institutional key management systems. It identifies applicable laws and directives concerning security planning and management, and suggests approaches to satisfying those laws and directives with a view to minimizing the impact of management overhead on organizational resources and efficiency. This guideline acknowledges that planning and documentation requirements associated with small scale or single system cryptographic applications will not need to be as elaborate as those required for large and diverse government agencies supported by a number of general support systems and major applications. However, any organization that employs cryptography to provide security services is required to have policy, practices and planning documentation at some level or number of levels.

Part 2 of the Recommendation for Key Management first identifies the structural and functional elements common to effective key management systems; second, identifies security planning requirements, general security policies and practices necessary to effective institutional key management; and finally, offers suggestions regarding how key management policies and procedures might be incorporated into security planning documentation that is already required by various Federal laws and directives.

Barker, W.C., Dray, J., Chandramouli, R., Schwarzhoff, T., Polk, T., Dodson, D., Mehta, K., Gupta, S., Burr, W., Grance, T., *Personal Identity Verification of Federal Employees and Contractors*, Federal Information Processing Standard (FIPS) 201, http://csrc.nist.gov/publications/fips/index.html, February 2005

FIPS 201 specifies the technical and operational requirements for interoperable PIV systems that issue smart cards as identification credentials and that use the cards to authenticate an individual's identity. FIPS 201 has been issued in two parts to allow for a smooth migration to a secure, reliable personal identification process. The first part of FIPS 201 (PIV I) describes the minimum requirements needed to meet the control and security objectives of HSPD 12, including the process to prove an individual's identity. The second part (PIV II) of FIPS 201 explains the many components and processes that will support a smart-card-based platform, including the PIV card and card and biometric readers. The specifications for PIV components support interoperability between components in systems and among the different department and agency systems. FIPS 201 responds to Homeland Security Presidential Directive (HSPD) 12, issued by President Bush on August 27, 2004, which cited the wide variations in the quality and security of the forms of identification used to gain access to federal and other facilities, and called for the development of a mandatory standard for secure and reliable forms of identification to be used throughout the federal government. The directive stated the government's requirements for a common government-wide identification system that would enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy. The FIPS was approved by Carlos M. Gutierrez, the U.S. Secretary of Commerce, on February 25, 2005.

Barker, W.C., *E-Government Security Issues and Measures*, Handbook of Information Security, John Wiley & Sons, Hossein Bidgoli (ed.), California State University at Bakersfield, to be published

The Handbook will be a three-volume, 2,400-page reference source providing state-of-the-art information concerning the information, computer and network security with coverage of the core topics. The audience is four-year colleges and universities with Computer Science, MIS, IT, IS, E-commerce, and Business departments, and public, private, and corporate libraries and a diverse group of professionals interested in this fast-growing field. The Handbook will be available as a printed work as well as in an online version. Approximately 200 articles will comprise this publication. This chapter identifies current security issues associated with implementation of E-Government initiatives and the security measures needed for, and available to, address these issues. The set of E-Government services that this chapter treats includes electronic publishing, interactive information services, transaction processing, and delivery of government services. The classes of security issues addressed include availability, integrity, confidentiality, and privacy. Security measures discussed include security mechanisms (e.g., cryptography, firewalls, and operating system security), system design and configuration principles (e.g., hardware, software, and data backups), and policy and procedural measures (e.g., planning, testing, certification, monitoring/auditing, and accreditation).

Bebu, I., Rukhin, A.L., *Stationary Distributions in the Atom-on-Demand Problem*, Probability in Engineering and Physical Sciences, to be published

In this note a probability model for the number of atoms in a magneto-optical trap is suggested. We study an ergodic Markov Chain for the number of atoms in the trap under a feedback regime for different load distributions. Formulas for the stationary distribution of the process are derived in several cases. They can be used to adjust the loading rate of atoms to maximize the probability of a single atom in the trap. The (approximate) optimal regimes are also found.

Beichl, I., Bullock, S., Song, D., *A Quantum Algorithm Detecting Concentrated Maps*, NIST Journal of Research (to be published), http://math.nist.gov/quantum/

Let for , some number of quantum bits. Using calls to a classical oracle evaluating and an -bit memory, it is possible to determine whether is one-to-one. For some radian angle , we say is -concentrated iff for some given and any . This manuscript presents a quantum algorithm that distinguishes a -concentrated from a one-to-one in calls to a quantum oracle function with high probability. For radians, the quantum algorithm outperforms the obvious classical algorithm on average, with maximal outperformance at radians. Thus, the constructions generalize Deutsch's algorithm, in that quantum outperformance is robust for (slightly) nonconstant .

Beichl, I., Sullivan, F., *The Other Monte Carlo Method*, IEEE Computing in Science and Engineering, to be published

This is a general article on a Monte Carlo method different from the traditional Metropolis algorithm. Sampling is done according to a non-uniform probability distribution that is generated as the choice is being made.

Bernal, J., Witzgall, C., *Integer Representation of Decimal Numbers for Exact Computations*, NISTIR 7144, http://math.nist.gov/~JBernal/JBernal_Pub.html

A scheme is presented and software is documented for representing as integers input decimal numbers that have been stored in a computer as double precision floating point numbers and for carrying out multiplications, additions and subtractions based on these numbers in an exact manner. The input decimal numbers must not have more than nine digits to the left of the decimal point. The decimal fractions of their floating point representations are all first rounded off at a prespecified location, a location no more than nine digits away from the decimal point. The number of digits to the left of the decimal point for each input number besides not being allowed to exceed nine must then be such that the total number of digits from the leftmost digit of the number to the location where round-off is to occur does not exceed fourteen.

Black, P.E., *Software Assurances Metrics and Tool Evaluation*, Proceedings of 2005 International Conference on Software Engineering Research and Practice, Las Vegas, Nevada, June 27-30, 2005

NIST is starting two ambitious projects to (1) develop a taxonomy of software security flaws and vulnerabilities, (2) develop a taxonomy of software assurance (SA) functions and techniques which detect those flaws, (3) perform and maintain a survey of SA tools implementing the functions, (4) develop testable specifications of SA functions and explicit tests, include a standard reference dataset, to evaluate how closely tools implement the functions, and (5) lead efforts to develop metrics for the effectiveness of those functions. The end result is that users will be able to choose a combination of techniques which best suits their needs and will be able to state how much confidence they have in software which has been assessed. This paper details these two projects and presents our justifications and expectations.

Black, P.E., *Software Write Block, Testing Support Tools Validation – Part A – Test Plan, Test Design, and Test Case Specification*, NISTIR 7207-A, http://www.cftt.nist.gov/swbTT%20A%20Validation3.pdf, May 2005

This NIST Internal Report consists of two parts. Part A covers the planning, design, and specification of testing and reviewing the Software write block (SWB) support tools. Part B, which is a companion document, covers the test and code review support report. Part A gives a test plan, test design specification, and test case specification for validation of the disk drive software write block testing support tools. The test plan defines the scope, including specific items and features to be validated, the methodology or approach for validating the SWB test support tools, and some technical background. The test design specification gives requirements for validating SWB tools. These requirements yield assertions. Each assertion leads to one or more code reviews or test cases consisting of preconditions, values, and method(s) for gaining confidence that the SWB test support tools correctly assess those assertions, a test procedure and the expected results. The test case specification gives details of test and review procedures for setting up the test, performing the test, and assessing the results. Appendices include a code review checklist and source code for validation programs. Part B reports the results of reviewing the source code of the SWB test tools and testing them against Part A of the companion NIST Internal Report entitled Software Write Block Testing Support Tools validation – Test Plan, Test Design Specification, and Test Case Specification.

Black, P.E., *Software Write Block, Testing Support Tools Validation – Part B – Test and Code Review Report*, NISTIR 7207-B, http://www.cftt.nist.gov/swbTT%20B%20Valid%20Report3.pdf, May 2005

This NIST Internal Report consists of two parts. Part A covers the planning, design, and specification of testing and reviewing the Software write block (SWB) support tools. Part B, which is a companion document, covers the test and code review support report. Part A gives a test plan, test design specification, and test case specification for validation of the disk drive software write block testing support tools. The test plan defines the scope, including specific items and features to be validated, the methodology or approach for validating the SWB test support tools, and some technical background. The test design specification gives requirements for validating SWB tools. These requirements yield assertions. Each assertion leads to one or more code reviews or test cases consisting of preconditions, values, and method(s) for gaining confidence that the SWB test support tools correctly assess those assertions, a test procedure and the expected results. The test case specification gives details of test and review procedures for setting up the test, performing the test, and assessing the results. Appendices include a code review checklist and source code for validation programs. Part B reports the results of reviewing the source code of the SWB test tools and testing them against Part A of the companion NIST Internal Report entitled Software Write Block Testing Support Tools validation – Test Plan, Test Design Specification, and Test Case Specification.

Blanz, V., Grother, P., Phillips, P. J., Vetter, T., *Face Recognition Based on Frontal Views Generated from Non-Frontal Images*, IEEE Conference on Computer Vision and Pattern Recognition 2005

This paper presents a method for face recognition across large changes in viewpoint. Our method is based on a Morphable Model of 3D faces that represents face-specific information extracted from a dataset of 3D scans. For non-frontal face recognition in 2D still images, the Morphable Model can be incorporated in two different approaches: In the first, it serves as a preprocessing step by estimating the 3D shape of novel faces from the non-frontal input images, and generating frontal views of the reconstructed faces at a standard illumination using 3D computer graphics. The transformed images are then fed into state of-the-art face recognition systems that are optimized for frontal views. This method was shown to be extremely effective in the Face Recognition Vendor Test FRVT 2002.

In the process of estimating the 3D shape of a face from an image, a set of model coefficients are estimated. In the second method, face recognition is performed directly from these coefficients. In this paper we explain the algorithm used to preprocess the images in FRVT 2002, present additional FRVT 2002 results, and compare these results to recognition from the model coefficients.

Bowdrey, M.D., Jones, J.A., Knill, E., Laflamme, R., *Compiling Gate Networks on an Ising Quantum Computer*, Physical Review A and http://arxiv.org/quant-ph, January 2005

Here we describe a simple mechanical procedure for compiling a quantum gate network into the natural gates (pulses and delays) for an Ising quantum computer.

Boyar, J., Peralta, R., *The Exact Multiplicative Complexity of the Hamming Weight Function*, Latin American Theoretical Informatics Symposium, 2006 (proceedings published by Springer-Verlag), to be published

We consider the problem of computing the Hamming weight of an n-bit vector using a circuit with gates for addition and multiplication modulo 2 (alternatively, XOR and conjunction gates) only. The number of multiplications necessary and sufficient to build such a circuit is called the "multiplicative complexity" of the Hamming weight function. We prove the exact multiplicative complexity of the Hamming weight function on n variables is n minus the Hamming weight of the binary representation of n.

Branstad, D.K., Clay, A., Hash, J., *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, NIST SP 800-79, http://csrc.nist.gov/publications/nistpubs/index.html, July 2005

Homeland Security Presidential Directive 12 (HSPD-12), entitled "Policy for a Common Identification Standard for Federal Employees and Contractors," established a policy for all Federal departments and agencies to create and use a government-wide secure and reliable form of identification for their Federal employees and contractors. It further specified that this secure and reliable form of identification be issued only by service providers whose reliability has been established by an official accreditation process. This document should be used by any Federal department or agency to accredit the reliability of the organization that will issue Personal Identity Verification (PIV) Cards that comply with Federal Information Processing Standard (FIPS) 201 to their Federal employees or Federal contractor employees. This document describes a set of attributes that should be exhibited by a PIV Card Issuing organization (hereafter called a PCI) in order to be accredited and should be used for assessing the reliability of an organization providing PCI services to a Federal agency or contractor. Certification in this context means a formal process of assessing the attributes affecting reliability of a PCI using various methods of assessment (e.g., interviews, laboratory test results, procedure evaluation) that support the assertion that the PCI is reliable and capable of enrolling approved Federal identity card applicants and issuing them PIV Cards. Accreditation is the official management decision of a Senior Agency Official to authorize operation of a PCI after determining that its reliability has satisfactorily been established through appropriate assessment and certification processes. Accreditation provides a form of quality control and helps to assure that the managers and technical staffs at all levels of a PCI will implement and perform procedures compliant with FIPS 201.

Brewer, T.L., Editor, *Computer Security Division 2004 Annual Report*, NISTIR 7219, http://csrc.nist.gov/publications/nistir/index.html, April 2005

This report covers the work conducted within the National Institute of Standards and Technology's Computer Security Division during Fiscal Year 2004. It discusses all projects and programs within the Division, staff highlights, and publications. For many years, the Computer Security Division (CSD) has made great contributions to help secure the nation's sensitive information and information systems. CSD's work has paralleled the evolution of information technology, initially focused principally on mainframe computers, to now encompass today's wide gamut of information technology devices. CSD's important responsibilities were re-affirmed by Congress with passage of the Federal Information Security Management Act of 2002 (FIMSA) and the Cyber Security Research and Development Act of 2002. Beyond the role to serve the Federal agencies under FISMA, CSD standards and guidelines are often voluntarily used by U.S. industry, global industry, and foreign governments as sources of information and direction for securing information systems. CSD's research also contributes to securing the nation's critical infrastructure systems. Moreover, the Division has an active role in both national and international standards organizations in promoting the interests of security and U.S. industry.

Bullock, S.S., Carteret, H.A., *Quantum Interferometer Circuits for Multi-Partite Entanglement*, Quantum Information and Computation, to be published

The concurrence of a pure quantum state of qubits is the component of the state vector on its spin-flip. In two qubits, it is equivalent to all other measures of entanglement, in particular a one-to-one function of the entropy of either partial trace. In the multi-partite case, any even-qubit state with a nonzero concurrence is not local but rather entangled. Here, we present quantum interferometer circuits which measure the entanglement (concurrence) of their quantum data registers. Computing the concurrence requires a sequence of such interferometers, and they function properly on mixed as well as pure even-qubit data-states.

Bullock, S.S., O'Leary, D.P., Brennen, G.K., *Asymptotically Optimal Quantum Circuits for d-level Systems*, Physical Review Letters 94 (2005), p. 230502, http://math.nist.gov/quantum/

As a qubit is a two-level system whose state space is spanned by and , so a qudit is a -level system whose state space is spanned by ,…, . Quantum computation has stimulated much recent interest in algorithms factoring unitary evolutions of an -qubit state space into component two-particle unitary evolutions. In the absence of symmetry, Shende, Markov, and Bullock use Sard's theorem to prove that at least two-qubit unitary evolutions are required, while Vartiainen, Moettoenen, and Salomaa (VMS) use the matrix factorization and Gray codes in an optimal order construction involving two-particle evolutions. In this work, we note that Sard's theorem demands two-qudit unitary evolutions to construct a generic (symmetry-less) -qudit evolution. However, the VMS result applied to virtual qubits only recovers optimal order in the case that is a power of two. We further construct a decomposition for multi-level quantum logics, proving a sharp asymptotic of two-qudit gates and thus closing the complexity question for all -level systems (finite). Gray codes are not required.

Burns, T.J., Schmitz, T.L., *A Study of Linear Joint and Tool Models in Spindle-Holder-Tool Receptance Coupling*, Proceedings of IDETC/CIE 2005: ASME 2005 International Design Engineering Technical Conference & Computers & Information in Engineering Conference, Long Beach, California, September 24-28, 2005

The dynamics of a spindle-holder-tool (SHT) system during high-speed machining is sensitive to changes in tool overhang length. A well-known method for predicting the limiting depth of cut for avoidance of tool chatter requires a good estimate of the tool-point frequency response (FRF) of the combined system, which depends upon the tool length. In earlier work, a combined analytical and experimental method has been discussed, that uses receptance coupling substructure analysis (RCSA) for the rapid prediction of the combined spindle-holder-tool FRF. The basic idea of the method is to combine the measured direct displacement vs. force receptance (i.e., frequency response) at the free end of the spindle-holder (SH) system with calculated expressions for the tool receptances based on analytical models. The tool was modeled as an Euler-Bernoulli (EB) beam, the other three spindle-holder receptances were set equal to zero, and the model for the connection with the tool led to a diagonal matrix. The main conclusion of the earlier work was that there was an exponential trend in the dominant connection parameter, which enabled interpolation between tip receptance data for the longest and shortest tools in the combined SHT system. Thus, a considerable savings in time and effort could be realized for the particular SHT system. A question left open in the earlier work was: how general is this observed exponential trend? Here, to explore this question further, an analytical EB model is used for the SH system, so that all four of its end receptances are available, and the tool is again modeled as a free-free EB beam that is connected to the SH by a specified connection matrix, that includes nonzero off-diagonal terms. This serves as the "exact" solution. The approximate solution is once again formed by setting all but one SH receptance equal to zero, and the connection parameters are determined using nonlinear least squares software. Both diagonal and full connection matrices are investigated. The main result is that, for this system, in the case of a diagonal connecting matrix, there is no apparent trend in the dominant connecting spring stiffness with tool overhang length. However, in the full connecting matrix case, a general constant trend is observed, with some interesting exceptions.

Chandramouli, R., Eyuboglu, L., Mehta, K., *PIV Middleware and On-Card Application Conformance Test Guidance (SP 800-73 Compliance)*, NIST SP 800-85, http://csrc.nist.gov/publications/nistpubs/index.html

This document specifies the test plan, processes, derived test requirements, and detailed test assertions for testing the following: (a) PIV middleware (client application API conformance), (b) PIV on-card application (for conformance to card application card command interface), (c) PIV Data objects representation, and (d) PIV Authentication Use Cases. The test requirements are based on the specifications in NIST Special Publication 800-73, *Interfaces for Personal Identity Verification*.

Chandramouli, R., *Privacy Protection of Enterprise Information through Inference Analysis*, IEEE 6th International Workshop on Policies for Distributed Systems and Networks, Stockholm, Sweden

Ensuring that Disclosure of Information to outside entities is in conformance with the enterprise privacy policies is of utmost concern for all enterprises dealing with consumer information. The existing protection measures proposed for meeting this goal are inadequate. In this paper we present an approach in which the privacy label taxonomy is developed to classify information types in an enterprise by their privacy labels. Inference Analysis is performed on the information types using a Disjunctive Logic Programming technique to detect violations of privacy labeling semantics in various information types. The analysis also provides the technique to deal with such violations so as to achieve a violation-free privacy labeling scheme.

Chandramouli, R., Rose, S., *An Integrity Verification Scheme for DNS Zone File Based on Security Impact Analysis*, 21st Annual Computer Security Applications Conference, Tucson, Arizona

The Domain Name System (DNS) is the world's largest distributed computing system that performs the key function of translating user-friendly domain names to IP Addresses through a process called Name Resolution. After looking at the protection measures for securing the DNS transactions, we discover that the trust in the name resolution process ultimately depends upon the integrity of the data repository that Authoritative Name Servers of DNS uses. This data repository is called Zone file. Hence we analyze in detail the data content relationships in zone file that have security impacts and develop a taxonomy and associated population of constraints. We also have developed a platform-independent framework using XML, XML Schema and XSLT for encoding those constraints and verifying them against the XML encoded zone file data to detect integrity violations.

Chang, W., *Embedding MPEG-7 Metadata Within a Media File Format*, SPIE Conference, August 2005

Embedding metadata within a media file format becomes evermore popular for digital media. Traditional digital media files such as MP3 songs and JPEG photos do not carry any metadata structures to describe the media content until these file formats got extended with ID3 and EXIF. Recently both ID3 and EXIF advanced to version 2.4 and version 2.2 respectively with much added new description tags. Currently, most MP3 players and digital cameras support the latest revisions of these metadata structures as the de-facto standard formats. Given the benefits of having metadata to describe the media content is very critical to consumers for viewing and searching media content. However, both ID3 and EXIF were designed with very different approaches in terms of syntax, semantic, and data structures. Therefore, these two metadata file formats are not compatible and cannot be utilized for other common applications such as slideshow for playing MP3 music in the background and shuffle through images in the foreground. This paper presents the idea of embedding the international standard of ISO/IEC MPEG-7 metadata descriptions inside the rich ISO/IEC MPEG-4 file format container so that a general metadata framework can be used for images, audio, and video applications.

Chang, W., *MPEG-7: Standard Metadata for Multimedia Content*, SPIE Conference, August 2005

The XML metadata technology of describing media contents has emerged as a dominant mode of making media searchable both for human and machine consumptions. To realize this promise, many online Web applications are pushing this concept to its full potential. However, a good metadata model does require a robust standardization effort so that the metadata content and its structure can reach its maximum usage between various applications. An effective media content description technology should also use standard metadata structures especially when dealing with various multimedia contents. A new metadata technology called MPEG-7 content description has taken off from the ISO MPEG standards body with the charter of defining standard metadata to describe audiovisual content. This paper will give an overview of MPEG-7 technology and what impact it can bring forth to the next generation of multimedia indexing and retrieval applications.

Chevrollier, N., Golmie, N., *On the Use of Wireless Network Technologies in Healthcare Environments*, 5th Workshop on Applications and Services in Wireless Networks, Paris, France, July 2005, http://w3.antd.nist.gov/pubs05.shtml

In this article, we investigate the suitability of wireless technologies in healthcare/hospital environments. We focus on Wireless Personal Area Network technologies, namely, Bluetooth and the low-rate specifications described in the IEEE 802.15.4 standard. We evaluate the relevance of each technology for supporting medical applications and examine related scalability issues. Moreover, we consider heterogeneous wireless technology environments and quantify the interaction between Bluetooth devices and IEEE 802.15.4 devices when they operate in the same environment.

Chevrollier, N., Montavont, N., Golmie, N., *Handovers and Interference Mitigation in Healthcare Environments*, Military Communications Conference, MILCOM 2005, Atlantic City, New Jersey, October 17-21, 2005, http://w3.antd.nist.gov/pubs05.shtml

In this article, we consider candidate wireless technologies such as IEEE 802.11b, and IEEE 802.15.4 that can support medical and healthcare informatics applications. The main questions that we try to answer are: (1) Is there any potential for significant interference when these wireless technologies are present? (2) What are potential solutions to mitigate it? We consider a handover technique for IEEE 802.11b devices as an effective way to mitigate interference and improve performance. We propose the use of packet loss and retransmissions at layer 2 in order to trigger a WLAN access point handover. Performance for scenarios of interest is measured in terms of packet loss, packet retransmissions, and delay jitter.

Cotrell, D.L., McFadden, G.B., *Axial Flow Effects on the Stability of Circular Couette Flow with Viscous Heating*, Physics of Fluids, to be published

We consider flow between concentric circular cylinders driven jointly by a constant axial pressure gradient and rotation of one or both cylinders. In this work we account for viscous heating effects, and have computed critical values for the radius ratio and rotation rate ratio used in the recent experiments of White & Muller. The effects of gravity are neglected, while conductivity, the volumetric coefficient of thermal expansion, density, and constant pressure specific heat are taken to be constant. In this work we allow the viscosity to vary with temperature. The analysis extends previous results with no axial flow, and accounts for arbitrary disturbances of infinitesimal amplitude. Results show that over the entire range of axial flow rates considered, stability boundaries differ significantly from those found for the zero axial flow case. Consistent with the isothermal results of Cotrell, Rani & Pearlstein and the non-isothermal results of Cotrell & McFadden, the critical disturbance is axisymmetric over only a finite range of Reynolds numbers beginning at zero, beyond which the critical disturbance becomes non-axisymmetric.

Cowley, P., Nowell, L., Scholtz, J., *Glass Box: An Instrumented Infrastructure for Supporting Human Interaction with Information*, Hawaii International Conference on System Science (HICSS 38), January 3, 2005

In this paper, we discuss the challenges involved in developing an infrastructure to support a new generation of analytic tools for information analysts. The infrastructure provides data for establishing context about what the analyst is doing with the analytic tools, supports an integration environment to allow suites of tools to work together, and supports evaluation of the analytic tools. We discuss the functionality of the Glass Box, the challenges of evaluating adaptive systems including the capture of data for evaluation metrics, and lessons learned from our experiences to date.

Cypher, D., Chevrollier, N., Montavont, N., Golmie, N., *Prevailing Over Wires in Healthcare Environments: Benefits and Challenges*, IEEE Communications Magazine Issue on Wireless Technology Advances and Challenges for Telemedicine (February 2006), to be published

The objectives of this article are to survey the benefits and challenges that poise the deployment and operation of wireless communications in support of healthcare networks. While the main advantages of wireless communications remain to provide ubiquitous connectivity including allowing greater physical mobility and interoperability, a number of engineering issues need to be addressed before this vision is realized. Our intent in this article is to explore some of these issues including deployment, interference, and mobility and provide insights for potential solutions.

Dabrowski, C., Mills, K.L., Quirolgico, S., *A Model-Based Analysis of First-Generation Service Discovery Systems*, NIST SP 500-260, http://www.antd.nist.gov/pubs/SP500_260final.pdf, October 2005

Future commercial software systems will be based on distributed service-oriented architectures in which applications are composed dynamically from remote components. A key part of service-oriented computing is the ability for clients to discover remote services that fulfill specific requirements. Since the mid-1990s, various commercial and public domain designs for service discovery systems have been proposed that enable clients and services to rendezvous in a distributed system. The report characterizes such designs as first-generation service discovery systems, based on the belief that experience with these systems will lead to future, improved designs.

Using three widely used service discovery systems as a basis, this publication first presents a high level overview of the operation of service discovery protocols. A detailed generic model of first-generation service discovery systems, written in UML, follows this. The UML model provides an in-depth analysis of the alternative service discovery designs available today, including the major functional components that comprise these designs, the behaviors of these components, and the information they exchange. The report verifies the generality of the model by mapping its component element to corresponding elements of existent and emerging service discovery systems. This report also identifies issues that designers should attempt to resolve in the next generation of service discovery systems.

The analysis is then extended to provide designers of future service discovery systems with a means to evaluate designs. First, the report proposes a set of service goals that service discovery systems should strive to satisfy to ensure a desirable level of quality of service. These goals provide a basis to define metrics, for evaluation the behavior and measuring performance of system designs and implementations. Second, the report identifies potential performance issues that may arise during operation of service discovery systems. Identifying performance issues can alert designers and implementers to the potential for unexpected behavior when service discovery technology is deployed at large scale. The report presents possible solutions to performance problems that extend well-known optimization algorithms for distributed systems and present new algorithms tailored to service discovery environments.

The contributions in this report will help to improve the quality of the next generation of service discovery systems on which the service-oriented architectures of tomorrow appear likely to depend. Further, should an industry standards group choose to develop a unified specification for service discovery, the model should provide helpful input to the process.

Dang, H.T., Palmer, M.S., *The Role of Semantic Roles in Disambiguating Verb Senses*, Proceedings of the 43rd Annual Meeting of the Association for Computational Linguistics

We describe an automatic Word Sense Disambiguation (WSD) system that disambiguates verb senses using syntactic and semantic features that encode information about predicate arguments and semantic classes. Our system performs better than the best published results on the English verbs of senseval-2. We also experiment with using the gold-standard predicate-argument labels from PropBank to disambiguate fine-grained WordNet senses and course-grained PropBank framesets, and show that WSD can be further improved with better extraction of semantic roles.

Davis, R.A., Dunsmuir, W.T.M., Streett, S.B., *Maximum Likelihood Estimation for an Observation Driven Model for Poisson Counts*, Methodology and Computing in Applied Probability, accepted for publication

This paper is concerned with an observation driven model for time series of counts whose conditional distribution given past observations follows a Poisson distribution. This class of models is capable of modeling a wide range of dependence structures and is readily estimated using an approximation to the likelihood function. Recursive formulae for carrying out maximum likelihood estimation are provided and the technical components required for establishing a central limit theorem of the maximum likelihood estimates are given in a special case.

DerSimonian, R., Kacker, R., *Random-Effects Model for Meta-analysis of Clinical Trials: An Update*, Controlled Clinical Trials, to be published

The random-effects model is a useful approach for meta-analysis of clinical studies. It explicitly accounts for the heterogeneity of studies through a statistical parameter representing the inter-study variation. We discuss several iterative and non-iterative alternative methods for estimating the inter-study variance and hence the overall population treatment effect. We show that the leading methods for estimating the inter-study variance are special cases of a general method-of-moments estimate of the inter-study variance. The general method suggests two new two-step methods. The iterative estimate is statistically optimal and it can be easily calculated on a spreadsheet program, such as Microsoft Excel, available on the desktop of most researchers. The two-step methods are useful when a non-iterative estimate is desired.

Diepold, K., Pereira, F., Chang, W., *MPEG-A: A Step Forward in MPEG Standardization*, IEEE Multimedia, Issue 3 for July-August 2005

MPEG standards are shaping the multimedia landscape since the beginning of the nineties. After the MPEG-1, MPEG-2, and MPEG-4 multimedia coding standards, the MPEG-7 content description standard and the MPEG-21 multimedia framework standard, MPEG is taking another step forward to impact the multimedia market. The MPEG-A standard targets the specification of Multimedia Application Formats, which are a class of 'super-formats' defined across MPEG standards or parts of standards; these super-formats target the provision of an additional level of interoperability on the application level, satisfying the growing need of users for more integrated solutions.

Donnelly, D., Rust, B.W., *The Fast Fourier Transform for Experimentalists, Part I: Concepts*, Computing in Science and Engineering 7(2), March/April 2005, pp.80-88.

The discrete Fourier transform (DFT) is a widely used tool for the analysis of measured time series data. The Cooley-Tukey fast Fourier transform (FFT) algorithm gives an extremely fast and efficient implementation of the DFT. This is the first of a series of three articles which will describe the use of the FFT for experimental practitioners. This installment gives fundamental definitions and tells how to use the FFT to estimate power and amplitude spectra of a measured time series. It discusses the use of zero padding, the problem of aliasing, the relationship of the inverse DFT to Fourier series expansions, and the use of tapering windows to reduce the sidelobes on the peaks in an estimated spectrum.

Donnelly, D., Rust, B.W., *The Fast Fourier Transform for Experimentalists Part II: Methods I*, Computing in Science and Engineering 7(4), July/August 2005, pp. 92-95.

This paper is the second in a series of tutorial essays on applications of the fast Fourier transform to the analysis of measured time series data. It continues the discussion of classical methods of spectral analysis which was started in Part I with the periodogram. It introduces the autocorrelation function and describes the correlogram methods that are based on both the biased and unbiased autocorrelation estimators. It describes the effects of truncating and/or tapering those estimators with various window functions. It also describes how the fast Fourier transform is used to rapidly calculate convolutions for two time series.

Dray, J.F., Guthery, S., Schwarzhoff, T., *Interfaces for Personal Identity Verification*, NIST SP 800-73, http://csrc.nist.gov/publications/nistpubs/index.html, April 2005

FIPS 201, Personal Identity Verification for Federal Employees and Contractors, specifies that the identity credentials must be stored on a smart card. Special Publication 800-73 contains technical specifications for smart card interfaces used to retrieve and use identity credentials. These specifications reflect the design goals of interoperability and PIV Card functions. The goals are addressed by specifying PIV data model, communication interface, and application programming interface (API). SP 800-73 enumerates requirements where the standards include options and branches and also constrain implementers' interpretation of the standards. Such restrictions are designed to ease implementation, facilitate interoperability, and ensure performance, in a manner tailored for PIV applications. Specifications include the PIV data model, API, and card interface requirements necessary to comply with the mandated use cases for interoperability across deployments or agencies. Interoperability is defined as the use of PIV identity credentials such that client APIs, compliant card applications and compliant integrated circuit cards can be used interchangeably by information processing systems across Federal agencies. SP 800-73 does not address the back-end processes that must be performed to attain full identity assertion. The document describes two realizations of the client-application programming and card command interfaces for personal identity verification: the transitional interfaces and the end-point interfaces. Transitional interfaces may be used by agencies with an existing identity card program as an optional step in evolving to the end-point interfaces. End-point interfaces are used by agencies without an existing identity card program and by agencies that elect to evolve to the end-point interface in one step rather than two. SP 800-73 is divided into three parts as follows: Part 1, providing the specification for that which is common to both the transitional and end-point interfaces and guidance on strategies for migrating from the transitional interfaces to the end-point interfaces; Part 2, describing the subsets of GSC-ISv2.1 that comprise the transitional interfaces to the PIV data model; and Part 3, describing in detail the end-point interfaces to the PIV data model.

Dworkin, M.J., *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, NIST SP 800-38B, http://csrc.nist.gov/publications/nistpubs/index.html, May 2005

This Recommendation specifies a message authentication code (MAC) algorithm based on a symmetric key block cipher. This block cipher-based MAC algorithm, called CMAC, may be used to provide assurance of the authenticity, and, hence, the integrity, of binary data.

Filliben, J.J., *Statistical Approaches in the NIST World Trade Center Analysis*, Proceedings of the 9th International Conference on Structural Safety and Reliability, Rome, Italy, June 19-23, 2005

The Federal Building and Fire Safety Investigation of the World Trade Center Disaster is currently essentially completed. The pre-collapse progression was extremely complicated, with structural, thermal, dynamic and stochastic interdependencies across time and space. Four pre-collapse stages (a simplification of reality) will be discussed: aircraft impact, fire spread, thermal propagation through insulation, and structural deformation. Engineering issues and the statistical methodologies to address them will be discussed. A major challenge in the statistical analysis of the World Trade Center was the relatively meager amount of data – little physical evidence remained that could shed light on important events occurring in the core of the WTC buildings. In this regard, the study was simultaneously assisted – and complicated – by reliance on computational engineering virtual data – primarily in the form of NIST FDS (Fire Dynamics Simulator) and phase-specific FEA (Finite Element Analysis) computational models. As analyses progress from component to subassembly to global models, such computational models require characterization and validation – it will be shown how experiment design played an important role in this regard. Various other statistical analysis techniques (e.g., complex demodulation for assessing post-impact building oscillation frequency and – indirectly – building damage) will also be discussed. This paper will emphasize the methodologies employed. Conclusions and recommendations resulting from the Federal Building and Fire Safety Investigation of the World Trade Center Disaster are presented in the investigation final report, due to be released in draft form in the Spring of 2005.

Fong, E., *Conformance Testing of the Government Smart Card*, NISTIR 7210, http://xw2k.sdct.itl.nist.gov/smartcard/, February 2005

A conformance Test suite helps to ensure consistency between a specification and the behavior of a product. This paper presents the conformance testing methodology for the Government Smart Card Interoperability Specification. It starts with some basic terminology in the area of testing and discusses a methodology on how to design conformance test. The test strategy used for the design of this conformance test suite uses the extended Markup Language (XML), which is a declarative, implementation-neutral markup language. Finally, the paper explores the benefits and limitations with the conformance testing approach for the Government Smart Card Interoperability Specification.

Fong, J.T., *A B C of Statistics for Verification and Validation (V & V) of Simulations of High-Consequence Engineering Systems*, Proceedings of 2005 ASME Pressure Vessels and Piping Division Conference, Denver, Colorado, July 17-21, 2005

We begin this expository essay by reviewing with examples what a typical engineer already knows about statistics. We then consider a central question in engineering decision making, i.e., given a computer simulation of high-consequence systems, how do we verify and validate (V & V) and what are the margins of errors of all the important predicted results?

To answer this question, we assert that we need three basic tools that already exist in statistical and metrological sciences: (A) Error Analysis. (B) Experimental Design. (C) Uncertainty Analysis. Those three tools, to be known as A B C of statistics, were developed through a powerful linkage between the statistical and metrological sciences. By extending the key concepts of this linkage from physical experiments to numerical simulations, we propose a new approach to answering the V & V question. The key concepts are: (1) Uncertainty as defined in ISO Guide to the Expression of Uncertainty in Measurement (1993). (2) Design of experiments prior to data collection in a randomized or orthogonal scheme to evaluate interactions among model variables. (3) Standard reference benchmarks for calibration, and inter-laboratory studies for "weighted" consensus mean.

To illustrate the need for and to discuss the plausibility of this metrology-based approach, two example problems are presented: (a) Twelve simulations of the deformation of a linearly elastic simple cantilever beam with end point load, and (b) the calculation of a mean time to failure for a uniformly-loaded, 100-column, and single-floor steel grillage on fire.

Fong, J.T., *The Role of Engineering Statistics in a Reference Benchmark Approach to Verification and Validation of Multi-Physics Simulations of High-Consequence Engineering Systems*, Proceedings of the Stanford Mechanics Symposium on "Applied Mechanics and Multi-Physics Simulations of High-Consequence Engineering Systems," Stanford University, California, April 18, 2005, pp. 169-216.

Three basic tools in engineering statistics are considered: (A) Error Analysis, (B) Experimental Design, and (C) Uncertainty Analysis. It is argued that engineers who use mathematical, statistical, or computational models to simulate "high-consequence" systems for design, manufacturing, construction, maintenance, and retrofitting, need (A), (B), and (C) to ensure the correctness of those models by verification and validation (V&V). To support this argument, we examine a novel approach to V&V by extending three ideas in metrological science to numerical simulations: (I-1) expression of uncertainty as defined in ISO 1993 Guide to the Expression of Uncertainty in Measurement, (I-2) design of experiments, and (I-3) reference benchmarks for calibration and interpretation of key comparison and inter-laboratory studies. To illustrate the role of engineering statistics in this new approach, we provide four specific examples: (a) the uncertainty analysis of a length measurement process using standard 50 mm gauge blocks, (b) the verification of 12 simulations of the deformation of a cantilever beam, (c) the verification and validation of 15 simulations of the unconstrained cylindrical bending of 1.0-mm-thick aluminum sheet, and (d) the calculation of a mean time to failure due to fire for a uniformly loaded 100-column single-floor steel grillage.

Fong, T., Nourbakhsh, I., Ambrose, R., Simmons, R., Schultz, A., Scholtz, J., *The Peer-to-Peer Human-Robot Interaction Project*, Space 05, American Institute of Aeronautics and Astronautics, to be published

The Peer-to-Peer Human-Robot Interaction (PEP-HRI) project is developing techniques to improve task coordination and collaboration between human and robot partners. Our hypothesis is that peer-to-peer interaction can enable robots to collaborate in a competent, non-disruptive (i.e., natural) manner with users who have limited training, experience, or knowledge of robotics. Specifically, we believe that failures and limitations of autonomy (in planning, in execution, etc.) can be compensated for using human-robot interaction. In this paper, we present an overview of P2P-HRI, describe our development approach and discuss our evaluation methodology.

Gallagher, L.J., Offutt, A.J., Cincotta, A.V., *Integration Testing of Object-Oriented Components Using Finite State Machines*, Software Testing, Verification, and Reliability (STVR) International Journal, to be published

In object-oriented terms, one of the goals of integration testing is to ensure that messages from objects in one class or component are sent and received in the proper order and have the intended effect on the state of external objects that receive the messages. This research extends an existing single-class testing technique to integration testing of multiple classes. The previous method models the behavior of a single class as a finite state machine, transforms that representation into a data flow graph that explicitly identifies the definitions and uses of each state variable of the class, and then applies conventional data flow testing to produce test case specifications that can be used to test the class. This paper extends those ideas to inter-class testing by developing flow graphs and tests for an arbitrary number of classes and components. It introduces flexible representations for message sending and receiving among objects and allows concurrency among any or all classes and components. Data flow graphs are stored in a relational database, and database queries are used to gather def-use information. This approach is conceptually simple, mathematically precise, quite powerful, and general enough to be used for traditional data flow analysis. This testing approach relies on finite state machines, database modeling and processing techniques, and algorithms for analysis and traversal of directed graphs. The paper presents empirical results of the approach applied to an automotive system.

Garris, M.D., Wilson, C.L., *NIST Biometric Evaluations and Developments*, NISTIR 7204, http://www.itl.nist.gov/iaui/894.03/pact/pact.html and Photonics for Port and Harbor Security Conference Proceedings, March 2005 Defense & Security Symposium, Orlando, Florida, February 9, 2005

This paper presents an R&D framework used by the National Institute of Standards and Technology (NIST) for biometric technology testing and evaluation. The focus of this paper is on fingerprint-based verification and identification. Since 9-11 the NIST Image Group has been mandated by congress to run a program for biometric technology assessment and biometric systems certification. Four essential areas of activity are discussed: 1.) developing test datasets, 2.) conducting performance assessment; 3.) technology development; and 4.) standards participation. A description of activities and accomplishments are provided for each of these areas. In the process, methods of performance testing are described and results from specific biometric technology evaluations are presented. This framework is anticipated to have broad applicability to other technology and application domains.

Gentile, C., *Sensor Location through Linear Programming with Triangle Inequality Constraints*, IEEE International Conference on Communications, Seoul, Korea, May 16-20, 2005

Interest in dense sensor networks due to falling price and reduced size has motivated research in sensor location in recent years. While many algorithms can be found in literature, no benchmark exists and most papers fail to compare their results to other competing algorithms. To our knowledge, the algorithm which achieves the best performance in sensor location uses semi-definite relaxation of a quadratic program to solve the sensor location. We propose solving the same program, however without relaxing the constraints, but rather transforming them into linear triangle inequality constraints. Our linear program ensures a tighter solution to the problem. We benchmark ours against the competing algorithm, and provide extensive experimentation to substantiate the robustness of our algorithm even in the presence of high levels of noise.

Gharavi, H., Yan, B., Gao, S., *Multiple Description Video Coding Scheme for Multiple Path Routing Networks*, 16th International Symposium on Personal Indoor and Mobile Radio Communications

This paper presents a packet-based multiple description (MD) video-coding scheme, which uses interlaced high signal to noise ratio (H-SNR) and low signal to noise ratio (L-SNR) coded frames to produce two bit-streams (descriptions). At the decoder, when both bit-streams are received a high quality video will be reconstructed. If either one of the bit-streams is received, a poorer but acceptable quality video can be reconstructed. In this approach, we also considered the mismatch between the encoding and decoding loops due to motion compensation if only one bit-stream is received. We first give the results of the rate distortion performance of our scheme assuming that only one description is received. We then present simulation results under packet loss circumstances, which are simulated by error pattern files from real-world IP networks and ad-hoc networks. It is shown that the proposed scheme has a superior performance when compared with other schemes such as single description (SD) MPEG-4 video coder, and MD coding using video redundancy coding (MDC-VRC).

Gharavi, H., Yan, B., *Receiver Sensitivity-Based Power Control in Ad-hoc Multihop CSMA/CA*, IEEE CAS Transactions, to be published

This paper aims at improving the power efficiency of the Carrier Sense Multiple Access/ Collision Avoidance (CSMA/CA) protocol for transmission of multimedia information over multihop wireless channels. Using a distance dependent propagation model, we first derive a set of requirements to optimize the received power at every node in an active route. We then propose a power control scheme, which is based on the receiver sensitivity adjustment mechanism. The receiver sensitivity approach aims at exploiting a tradeoff between the interference and the contention in accessing the shared medium. Utilizing our simulation testbed developed for real-time traffic, we have shown that the proposed scheme can significantly improve the link performance in multihop communications.

Gilsinn, D.E., *Discrete Fourier Series Approximation to Periodic Solutions of Autonomous Delay Differential Equations*, Proceedings of IDETC/CIE 2005: ASME 2005 International Design Engineering Technical Conference & Computers & Information in Engineering Conference, Long Beach, California, September 24-28, 2005

This paper describes the algorithmic details involved in developing high order Fourier series representations for periodic solutions to autonomous delay differential equations. Although, the final approximate Fourier coefficients are computed by way of a nonlinear minimization algorithm, the steps to set up the objective function are shown to involve a sequence of matrix-vector operations. By proper coordination these operations can be made very efficient so that high order approximations can easily be obtained. An example of the calculations is shown for a Van der Pol equation with unit delay.

Gilsinn, D.E., Potra, F.A., *Integral Operators and Delay Differential Equations*, Journal of Integral Equations and Applications, to be published

The monodromy operator of a linear delay differential equation with periodic coefficients is formulated as an integral operator. The kernel of this operator includes a factor formed from the fundamental solution of the linear delay differential equation. Although the properties of the fundamental solutions are known, in general there is no closed form for the fundamental solution. This paper describes a collocation procedure to approximate the fundamental solution before the integral operator is discretized. Using arguments on collectively compact operators, the eigenvalues of the discretized monodromy operator are shown to converge to the eigenvalues of the monodromy operator in integral form. The eigenvalues of the monodromy operator tell the stability of the linear delay differential equation.

Glancy, S.C., Knill, E., *Error Analysis for Encoding a Qubit in an Oscillator*, Physical Review A and http://arxiv.org/quant-ph

In [5], Gottesman, Kitaev, and Preskill described a method to encode a qubit in the continuous Hilbert space of an oscillator's position and momentum variables. This encoding provides a natural error correction scheme which can correct errors due to small shifts of the position or momentum wave functions (i.e. use of the displacement operator). We present bounds on the size of correctable shift errors when both qubit and ancilla states may contain errors. We then use these bounds to constrain the quality of input qubit and ancilla states.

Godil, A., Ressler, S., *Similarity Based Retrieval from a 3D Human Database*, Siggraph 2005 Poster

In this paper, we describe a framework for similarity based retrieval from a 3D human database. Our technique is based on both body and head shape representation and retrieval based on similarity of both of them. The 3D human database used in our study is the CAESAR anthropometric database and there are around 5000 bodies. Furthermore, we have developed a web based interface for specifying the queries and to interact with the retrieval system. We have seen that our approach performs the similarity based retrieval in reasonable amount of time and seems to be a practical approach.

Griffith, D., Sriram, K., Gao, J., Golmie, N., *Wireless Enhancements for Storage Area Networks*, IEEE International Conference on Broadband Networks (BROADNETS 2005), Boston, Massachusetts, October 3-7, 2005, http://w3.antd.nist.gov/pubs05.shtml

We propose the creation of a wireless storage area network (SAN) and analyze its benefits. The proposed wireless SAN (WSAN) consists of a SAN switch that is connected to multiple wireless access points (APs) that communicate with the storage devices. This network would save space and reduce overall costs by not requiring wired connections. Wireless SANS would also provide more freedom in the placement of storage devices. However, because the number of wireless access points is less than the number of storage devices, it is possible for user data requests to be blocked if all access points are busy. An important design goal is therefore to minimize the probability that a network access request will be blocked.

Griffith, D., Sriram, K., Golmie, N., *Protection Switching for Optical Bursts Using Segmentation and Deflection Routing*, IEEE Communications Letters 2005, http://w3.antd.nist.gov/pubs05.shtml

Burst segmentation in OBS networks can significantly reduce the amount of data that is lost due to contention events by dropping or deflecting only the portion of a burst that overlaps another contending burst. In this letter, we demonstrate how segmentation combined with deflection routing can be used to reduce the amount of data that is lost when network elements fail. By enabling an OBS switch to deflect the tail-end segments of bursts that are in transmission as soon as it becomes aware of a downstream link failure, the retransmission of lost data can be reduced.

Gurski, K.F., McFadden, G.B., Miksis, M.J., *The Effect of Contact Lines on the Rayleigh Instability with Anisotropic Surface Energy*, SIAM Journal on Applied Mathematics, to be published

We determine the linear stability of a rod or wire on a substrate subject to capillary forces arising from an anisotropic surface energy for a range of contact angles between $-\pi/2$ and $\pi/2$. The Unperturbed rod is assumed to have infinite length with a uniform cross-section given by a portion of the two-dimensional equilibrium shape. We examine the effect of surface perturbations on the total energy. The stability of the equilibrium interface is reduced to determining the eigenvalues of a coupled system of ordinary differential equations. This system is solved both asymptotically and numerically for several types of anisotropic surface energies. We find that, in general, the presence of the substrate has a stabilizing effect as compared to a free rod.

Hagwood, C., *Dynamic Calibration*, Journal of the American Statistical Society, Applications and Case Studies, to be published

The NIST Pressure Measurements Division provides calibration service for pressure instruments that customers in turn use to calibrate other instruments. Often during their useable lifetime, these instruments are calibrated and recalibrated several times at NIST. Ideally, if an instrument has not degraded too badly, then using the prior data should improve the calibration estimate. A dynamic linear model is used to provide an algorithm for incorporating prior calibration data into the calibration process. Using simulation data and data from the calibration of a pressure transducer it is shown that the prior data does indeed improve recalibration if the instrument’s drift is not too large.

Harman, D., *Text Retrieval Conference and Message Understanding Conference*, Encyclopedia of Language and Linguistics, to be published

The Text REtrieval Conferences (TRECs) and the Message Understanding Conferences (MUCs) are two critical evaluation efforts in natural language understanding that in large part have shaped the research in those areas during the 1990s. The TREC work concentrated on research in information retrieval, starting with the basic retrieval task of finding documents in response to a question, but then branching into multiple variations on this central theme. The MUC tests have targeted information extraction, in particular how to find and aggregate specific information on entities such as persons, locations, and organizations, and the relationships between such entities.

Harman, D., *The History of IDF and its Influences on IR and Other Fields*, Progress in Natural Language Processing & Information Retrieval: A Festschrift for Karen Sparck Jones

The surprisingly simple IDF measure developed in 1972 by Karen Sparck Jones has continued to dominate the term weighting metrics used in information retrieval, despite several efforts to develop more complex measures of term distribution. It has been incorporated in (probably) all information retrieval systems and used in languages other than English. This chapter presents the origins of the IDF measure and how it evolved into the measure that is used today.

Harman, D., *The Importance of Focused Evaluations: A Case Study of TREC and DUC*, Progress in Natural Language Processing & Information Retrieval: A Festschrift for Karen Sparck Jones

Evaluation has always been an important part of scientific research, and in information retrieval, this evaluation has mostly been done using test collections. In 1992, a new test collection was built at the National Institute of Standards and Technology (NIST), and a focused evaluation (the Text REtrieval Conference or TREC) was started to use the collection. Results from nearly 12 years of this focused evaluation show significant technology transfer across systems, leading to major improvements in system performance. Focused evaluations also create the ability to target specific problems in language technology, such as retrieval across languages, and to design tasks for evaluation such that issues can be studied concurrently by multiple groups. This chapter will discuss some of the tasks that have been examined in TREC, including critical factors in the design of those evaluations. Additionally a second focused evaluation, the Document Understanding Conference (DUC) which evaluates text summarization, will be discussed.

Harman, D., Voorhees, E.M., *TREC: An Overview*, Annual Review of Information Science and Technology, Volume 40

The Text REtrieval Conference (TREC) is a workshop series designed to build the infrastructure necessary for large-scale evaluation of text retrieval technology. Participants in the workshops (over 100 groups in the latest TREC) have been drawn from the academic, commercial, and government sectors, and have included representatives from more than 20 different countries. These collective efforts have accomplished a great deal: a variety of large test collections have been built for both traditional "ad hoc" retrieval and related tasks such as cross-language retrieval, speech retrieval, and question answering; retrieval effectiveness has approximately doubled; and many commercial retrieval systems now contain technology first developed in TREC. This chapter chronicles the first twelve years of TREC, with extensive references to the experiments that have been done during those years.

Hash, J., Bowen, P., Johnson, A., Smith, C.D., Steinberg, D.I., *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act*, NIST SP 800-66, http://csrc.nist.gov/publications/nistpubs/index.html, March 2005

This Special Publication summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule. This publication helps to educate readers about information security terms used in the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the Security Rule. This publication is also designed to direct

readers to helpful information in other NIST publications on individual topics the HIPAA Security Rule addresses. Readers can draw upon these publication for consideration in implementing the Security Rule. This publication is intended as an aid to understanding security concepts discussed in the HIPAA Security Rule and does not supplement, replace, or supersede the HIPAA Security Rule itself.

Hash, J., *Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, ITL Bulletin, http://csrc.nist.gov/publications/nistbul/index.html, April 2005

This ITL Bulletin helps to educate readers about the HIPAA Security Rule and to improve understanding of the meaning of the security standards set out in the Security Rule. This publication is also designed to direct readers to helpful information in other NIST publications on individual topics the HIPAA Security rule addresses. Readers can draw upon these publications for consideration in implementing the Security Rule. This publication is intended as an aid to understanding security concepts discussed in the HIPAA Security Rule, and does not supplement, replace, or supersede the HIPAA Security Rule itself.

Hash, J., *Integrating IT Security into the Capital Planning and Investment Control Process*, ITL Bulletin, http://csrc.nist.gov/publications/nistbul/index.html, January 2005

To assist federal agencies with effectively integrating security into the capital planning and investment control (CPIC) process, NIST has released Special Publication (SP) 800-65, Integrating IT Security into the Capital Planning and Investment Control Process. It provides tips and pointers in addition to a sample methodology, which can be used to address prioritization of security requirements in support of agency business units. The publication describes risk factors which should be considered in addressing security investments and links the current Office of Management and Budget (OMB) guidance in this area to the current Federal Information Security Management Act (FISMA) including the Plan of Action and Milestones (POA&M) process which all agencies are required to implement. NIST Special Publication 800-65 describes in detail the underpinning methodology which can be easily applied to address security requirement integration and prioritization into an agency's capital planning and investment planning process using well understood concepts related to the current FISMA framework and existing NIST standards and guidance. This ITL Bulletin summarizes the special publication.

Hash, J., *Integrating IT Security into the Capital Planning and Investment Control Process*, NIST SP 800-65, http://csrc.nist.gov/publications/nistpubs/index.html, January 2005

Traditionally, information technology (IT) security and capital planning and investment control (CPIC) processes have been performed independently by security and capital planning practitioners. However, the Federal Information Security Management Act (FISMA) of 2002 and other existing federal regulations charge agencies with integrating the two activities. In addition, with increased competition for limited federal budgets and resources, agencies must ensure that available funding is applied towards the agencies' highest priority IT security investments. Applying funding towards high-priority security investments supports the objective of maintaining appropriate security controls, both at the enterprise-wide and system level, commensurate with levels of risk and data sensitivity. This special publication (SP) introduces common criteria against which agencies can prioritize security activities to ensure that corrective actions identified in the annual FISMA reporting process are incorporated into the capital planning process to deliver maximum security in a cost-effective manner.

Hewett,T.T., Scholtz, J.C., *A Questionnaire to Assess the Difficulty of Open Source Analysis Taskings*, 2005 International Conference on

Intelligence Analysis

Our goal is to produce metrics for assessing the impact of software tools and environments produced for the intelligence community. To this end we are developing a task difficulty questionnaire to attempt to identify and assess the impact of task characteristics that make some open source analytic taskings harder than. In this paper we present the most recent version of the questionnaire and invite comments and suggestions for improvement.

Hewett,T.T., Scholtz, J.C., *Developing a Difficulty Metric for Open Source Analytic Tasks*, 2005 International Conference on Intelligence Analysis

Our goal is to produce metrics for assessing the impact of software tools and environments produced for the intelligence community. To this end we need to understand the variables that make some analytic tasks harder than others and to determine which data need to be captured to meaningfully assess the effects of these variables on process and effectiveness. In this paper we describe the initial stages of development of a task difficulty questionnaire and report some feedback on the questionnaire collected from professional intelligence analysts in the context of their work. We discuss some additional steps needed to further clarify and refine the task difficulty questionnaire and explore the implications for possible task difficulty metrics.

Hicklin, R.A., Watson, C.I., Ulery, B., *The Myth of the Goats: How Many People Have Fingerprints that are Hard to Match?*, NISTIR, to be published

The proportion of people who have fingerprints that are particularly hard to match (also known as "Goats") is a topic of great interest in biometrics, especially for those involved in the design, development, or evaluation of fingerprint-based identification or verification systems. There have been a variety of statements made in the recent past that a small percentage of people (usually 2 %) cannot be fingerprinted due to poor quality fingers. This study shows these statements are based on misconceptions: the fact that some small percentage of fingerprints may be hard to match does not mean that a corresponding percentage of people are hard to match.

Hornikova, A., Book Review for Technometrics: *Statistics for the Quality Control Chemistry Laboratory* by Eamonn Mullins, 2003.

Hornikova, A., Guthrie, W.F., *A Survey of Key Comparisons*, Proceedings of the Measurement Science Conference 2005, Anaheim, California, January 2005

Key Comparisons are international inter-laboratory studies used to establish the degree of equivalence between national measurement standards. These studies, carried out by National Metrology Institutes, are time-consuming, but necessary to facilitate international trade. Since the signing of the Mutual Recognition Arrangement (MRA) in 1999, approximately 120 Key Comparisons in a wide range of metrological areas have been completed and have results posted in the Key Comparison Database (KCDB) maintained by the International Bureau of Weights and Measures (BIPM) in France and in the International Comparisons Database (ICDB) maintained by the National Institute of Standards and Technology (NIST) in the U.S. As with many new standardized procedures, however, the translation of the guidelines for the conduct of Key Comparisons outlined in the MRA from theory to practice has not always been smooth or obvious. Different groups of metrologists working in different areas have interpreted the MRA in different ways. The practicalities of collecting data that support a specific measurement goal from laboratories all over the world has also had varying impact on the decisions made by the scientists who have planned and participated in Key Comparisons. Now, supported by a large set of completed comparisons from the KCDB and ICDB, an opportunity to study methods actually being used to conduct Key Comparisons have now arisen. This paper summarizes work on currently completed Key Comparisons and offers recommendations for the design, analysis, and interpretation of future comparisons.

Hornikova, A., Guthrie, W.F., *Troubleshooting Key Comparisons*, Proceedings of Joint Statistical Meetings 2004, Toronto, Canada, December 2004

Key Comparisons are international inter-laboratory studies used to establish the degree of equivalence between national measurement standards. These studies, carried out by National Measurement Institutes, are time-consuming, but necessary to facilitate international trade. Since the signing of the Mutual Recognition Arrangement (MRA) in 1999, approximately sixty Key Comparisons in a wide range of metrological areas have been completed and have results posted in the Key Comparison Database (KCDB) maintained by the International Bureau of Weights and Measures (BIPM) in France and in the International Comparisons Database (ICDB) maintained by the National Institute of Standards and Technology (NIST) in the U.S. As with many new standardized procedures, however, the translation of the guidelines for the conduct of Key Comparisons outlined in the MRA from theory to practice has not always been smooth or obvious. Different groups of metrologists working in different areas have interpreted the MRA in different ways. The practicalities of collecting data that support a specific measurement goal from laboratories all over the world has also had varying impact on the decisions made by the scientists who have planned and participated in Key Comparisons. Now, supported by a rich set of real comparisons from the KCDB and ICDB, an opportunity to study methods actually being used to conduct Key Comparisons has now arisen. This paper summarizes work on currently completed Key Comparisons and offers recommendations for the design, analysis, and interpretation of future comparisons.

Hornikova, A., Zhang, N.F., *The Relation between the En Values Including Covariance and the 'Exclusive' Statistic*, Metrologia, to be published

In this short communication, we are dealing with En values when taking into account the covariance and comparing them with the corresponding "exclusive" statistic within an inter-laboratory study. The simple conclusion from this analysis is that there are no differences between the   values accounting for covariance and the corresponding 'exclusive' statistic.

Hornikova, A., Zhang, N.F., Welch, M.J., Tai, S., *An Application of Combining Results from Multiple Methods -Statistical Evaluation of Uncertainty for NIST SRM 1508a*, NCSL International Conference 2005

NIST Standard Reference Materials (SRMs) are certified reference materials that are developed at NIST and provided to laboratories (industry, government and academia) for assessment and improvement of measurement quality. SRM 1508a is recertified to update values and was evaluated at the Statistical Engineering Division at NIST using several different statistical models. The recertification is based on combining of the measurement results in subsets at each level varying due to use of different measurement methods and/or years. For statistical analysis, we decided to treat levels separately and to consider each of five method/year combinations as individual subset. In this study, we considered several different statistical models and corresponding estimators for the certified value, its uncertainty and the corresponding 2 sigma coverage interval.

Huang, I-F., Hwang, I-S., Shie, H-J., *Guaranteed Quality of Recovery in WDM Mesh Networks*, IEEE Proceedings Communications Research Publication, 2005, to be published

This study proposes a mechanism of guaranteed quality of recovery (GQoR) for Wavelength Division Multiplexing (WDM) mesh networks. Four GQoR levels are used to support customized services, and each of them is mapped to the adaptive recovery methodology. Once a failure occurs, the control system activates the recovery mechanism in compliance with the GQoR level. If the protection procedure fails as well, the proposed algorithm will then execute the restoration mechanism. Consequently, the recovery success rate is increased. This paper examines the shared segment recovery methods to establish backup path; therefore, it is well suited for large-scale networks and also increases the bandwidth utilization of the networks. Furthermore, a node deals only with its own routing information by employing the distributed control, so the fault recovery procedure can be speeded up. Simulation results reveal that the proposed method has greater performance of lower blocking probability and mean hop number than other methods previously reported in the literature.

Hunt, F.Y., *A Pathwise Optimality Result For A Class of Unichain Markov Decision Processes*, Proceedings of a Workshop on Ergodic Theory & Probability Theory, American Mathematical Society, Chapel Hill, North Carolina, February 2004

In this paper, we will discuss Markov decision processes (MDPs). These are controlled Markov processes whose state process under any stationary policy is an ergodic Markov chain. We assume here that the state space is countable and the action space (the set of possible controls) is finite. The stationary policy that produces a long term expected average cost that is equal to or smaller than the corresponding cost associated with any other stationary policy is called optimal. When the state process is uniformly ergodic and the cost of a single choice of action and state are bounded, we show how this minimizing property can be extended to the actual sample path costs of a process controlled by an optimal policy. We close by describing the application to a problem in bioinformatics that motivated this investigation.

Hunt, F.Y., O'Gallagher, A., Sensitivity of Multiple Sequence Alignments to Perturbations in Cost Matrices, Technical Note

A description of a new method for aligning biological sequences is presented. It is based on a formulation as a Markov decision optimization problem. Alignment is obtained by solving an associated linear programming problem. In this paper we show that the sensitivity of the alignment to changes in the cost matrices can be quantified. This is in contrast to conventional dynamic programming based methods.

Hwang, I-S., Huang, I-F., Chien, C-D., Su, D., *Efficient Path-Segment Protection Utilizing Logical-ring Approach in WDM Mesh Network*, Institute of Electronics, Information and Communication Engineers (IEICE) Transactions on Information & Systems, 2006, to be published

This work proposes a distributed fault protection mechanism called the Dynamic-Shared Segment Protection (DSSP) algorithm for WDM (Wavelength Division Multiplexing) mesh networks. The study explores the shared protection scheme in the network with constraints of Shared Risk Link Group (SRLG) and Shared Bandwidth Assignment (SBA). The objects are to assure high probability of path protection and efficient use of network resources. The proposed approach exploits the segment protection mode, which accommodates the characteristics of both path-based and link-based protections, for providing finer service granularities, to satisfy the versatile requirements of critical applications in foreseeable future. The protection paths are pre-calculated from the logical-rings, which are dynamically created from mesh networks. Accordingly, the DSSP algorithm is able to select the suitable logical-rings to be protection paths quickly once a working path is assigned. To show that DSSP can improve performance efficiency, simulations are conducted using four networks (NSFNET, USANET, Mesh 6x6, Mesh 9x9) for a comparative study of the proposed DSSP versus ordinary shared protection schemes and SLSP (Short Leap Shared Protection). Simulation results reveal that the proposed DSSP method results in much lower blocking probability and has higher network utilization. Consequently, it is very useful for application to a real-time WDM network, which changes status dynamically.

Irvine, J.M., Fenimore, C.P., Cannon, D., Roberts, J., Israel, S A., Simon, L., Watts, C., Miller, J.D.; Avilés, A.I., Tighe, P.F., Behrens, R.J., *Factors Affecting Development of a Motion Imagery Quality Metric*, Proceedings Visual Information Processing Conference (SPIE Defense and Security Symposium 2005), Orlando, Florida, March 29-30, 2005

The motion imagery community would benefit from the availability of standard measures for assessing image interpretability. The National Imagery Interpretability Rating Scale (NIIRS) has served as a community standard for still imagery, but no comparable scale exists for motion imagery. Several considerations unique to motion imagery indicate that the standard methodology employed in the past for NIIRS development may not be applicable or, at a minimum, require modifications. Traditional methods for NIIRS development rely on a close linkage between perceived image quality, as captured by specific image interpretation tasks, and the sensor parameters associated with image acquisition. The dynamic nature of motion imagery suggests that this type of linkage may not exist or may be modulated by other factors. An initial study was conducted to understand the effects target motion, camera motion, and scene complexity have on perceived image interpretability for motion imagery. This paper summarizes the findings from this evaluation. In addition, several issues emerged that require further investigation: § The effect of frame rate on the perceived interpretability of motion imagery, § Interactions between color and target motion which could affect perceived interpretability,§ The relationships among resolution, viewing geometry, and image interpretability, and § The ability of an analyst to satisfy specific image exploitation tasks relative to different types of motion imagery clips. Plans are being developed to address each of these issues through direct evaluations. This paper discusses each of these concerns, presents the plans for evaluations, and explores the implications for development of a motion imagery quality metric.

Irvine, J.M., Fenimore, C.P., Cannon, D., Roberts, J., Israel, S.A., Simon, L., Watts, C., Miller, J.D., Avilés, A.I., Tighe, P.F., Behrens, R.J., *Feasibility Study for the Development of a Motion Imagery Quality Metric*, Proceedings of Applied Imagery Pattern Recognition Workshop 2004, Washington, D.C., October 13-15, 2004

The motion imagery community would benefit from the availability of standard measures for assessing image interpretability. The National Imagery Interpretability Rating Scale (NIIRS) has served as a community standard for still imagery, but no comparable scale exists for motion imagery. Several considerations unique to motion imagery indicate that the standard methodology employed in the past for NIIRS development may not be applicable or, at a minimum, require modifications. Traditional methods for NIIRS development rely on a close linkage between perceived image quality, as captured by specific image interpretation tasks, and the sensor parameters associated with image acquisition. The dynamic nature of motion imagery suggests that this type of linkage may not exist or may be modulated by other factors. An initial study was conducted to understand the effects of specific factors on perceived image interpretability for motion imagery. These factors are: Target motion: Other studies indicate that moving targets exhibit greater salience that can enhance target detection and recognition; Camera motion: The parallax effect and changing viewing geometry assist the analyst, particularly when viewing partially occluded targets; Scene complexity: It has been hypothesized that both target and camera motion exhibit greater effects on perceived interpretability when the scenes are more complex. In this evaluation, a number of experienced imagery analysts provided ratings and comparisons of a number of motion imagery clips and images derived from these clips. The image set was well characterized in terms of target motion, camera motion, and scene complexity, as well as ground sampled distance. Analysis of the data from this evaluation provides insight into the magnitude of these effects on perceived image interpretability. This paper describes the evaluation, presents the results, and explores the implications for development of a “NIIRS-like” scale for motion imagery.

Jansen, W.A., Ayers, R.P., *An Overview and Analysis of PDA Forensic Tools*, Digital Investigation, The International Journal of Digital

Forensics & Incident Response, Elsevier, to be published

Mobile handheld devices are becoming evermore affordable and commonplace in society. When they are involved in a security incident or crime, forensic specialists require tools that allow proper extraction and speedy examination of any digital evidence present. This paper gives an overview of forensic software tools for Personal Digital Assistants (PDA). A set of generic scenarios was devised to simulate evidentiary situations and applied to a set of target devices to gauge how selected tools react under various situations. The paper summarizes those results, giving a snapshot of the capabilities and limitations of present day tools, and also provides background information on PDA hardware and software.

Jansen, W.A., Ayers, R.P., *Guidelines on PDA Forensics, Recommendations of the National Institute of Standards and Technology*, NIST SP 800-72, http://csrc.nist.gov/publications/nistpubs/index.html, November 2004

Forensic specialists periodically encounter unusual devices and new technologies normally not envisaged as having immediate relevance from a digital forensics perspective. The objective of the guide is twofold: to help organizations evolve appropriate policies and procedures for dealing with Personal Digital Assistants (PDAs), and to prepare forensic specialists to deal with new situations when they are encountered. This guide provides an in-depth look into PDAs and explains associated technologies and their impact on the procedures for forensic specialists. It covers the characteristics of three families of devices: Pocket PC, Palm OS, and Linux based PDAs and the relevance of various operating systems associated.

Jansen, W.A., Gavrila, S.I., Korolev, V., *Proximity Beacons and Mobile Device Authentication: An Overview and Implementation*, NISTIR 7200, http://csrc.nist.gov/publications/nistir/index.html, June 2005

The use of mobile handheld devices within the workplace is expanding rapidly. These devices are no longer viewed as coveted gadgets for early technology adopters, but have instead become indispensable tools that offer competitive business advantages for the mobile workforce. While these devices provide productivity benefits, they also pose new risks to an organization's security by the information they contain or can access remotely.

Enabling adequate user authentication is the first line of defense against unauthorized use of an unattended, lost, or stolen handheld device. This report describes an innovative type of authentication mechanism that relies on the presence of a signal from a wireless beacon for access to be granted. Such proximity beacons can be either organizational or personal oriented, and require only that handheld devices support a common standard wireless interface for Personal Area Network (PAN) communications, such as Bluetooth. Details of the design and implementation for both personal and organizational proximity beacons are provided.

Jansen, W.A., Gavrila, S.I., Korolev, V., *Proximity-Based Authentication for Mobile Devices*, 2005 International Conference on Security and Management, Las Vegas, Nevada, June 20-23, 2005

While mobile handheld devices provide productivity benefits, they also pose new risks. User authentication is the best safeguard against the risk of unauthorized use and access to a device's contents. This paper describes two location-based user authentication mechanisms designed to take advantage of Bluetooth functionality built into many current handheld devices.

Jansen, W.A., Gavrila, S.I., Séveillac, C., Korolev, V., *Smart Cards and Mobile Device Authentication: An Overview and Implementation*, NISTIR 7206, http://csrc.nist.gov/publications/nistir/index.html, July 2005

The use of mobile handheld devices within the workplace is expanding rapidly. These devices are no longer viewed as coveted gadgets for early technology adopters, but have instead become indispensable tools that offer competitive business advantages for the mobile workforce. While these devices provide productivity benefits, they also pose new risks to an organization's security by the information they contain or can access remotely. Enabling adequate user authentication is the first line of defense against unauthorized use of an unattended, lost, or stolen handheld device. Smart cards have long been the choice of authentication mechanism for many organizations; however, few handheld devices easily support readers for standard-size smart cards.

This report describes two novel types of smart cards that use standard interfaces supported by handheld devices, avoiding use of the more cumbersome standard-size smart card readers. These solutions are aimed at helping organization apply smart cards for authentication and other security services. Details of the design and implementation are provided.

Kacker, R., Toman, G., Huang, D., *Comparison of ISO-GUM*, Draft GUM Supplement 1, and Bayesian Statistics Using Simple Linear Calibration, Metrologia

We compare three approaches for quantifying uncertainty using a measurement equation: the International Organization for Standardization (ISO) Guide to the Expression of Uncertainty in Measurement (GUM), draft GUM Supplement 1, and Bayesian statistics. We use the measurement equation for simple linear calibration as an illustration. It includes both TypeA and TypeB input variables. We consider three scenarios: (i) the measurement equation is linear. (ii) the measurement equation is non-linear and the TypeB input variables have normal distributions, and (iii) the measurement equation is non-linear and the Type B input variables have rectangular distributions. We consider both small and large uncertainties for the Type B input variables. We use each of the three approaches to quantify the uncertainty in measurement for each of the cases considered. Based on this study and the original publications, we discuss the merits and limitations of each approach.

Kacker, R.N., Datla, R.U., Parr, A.C., *Response to Comments by Franco Pavese on Kacker et al.*, Metrologia 41 (2004) 340-352, Metrologia 42 (2005), pp. L13-L14.

This is response to comments on our published papers submitted by Dr. Franco Pavese of the NMI of Italy.

Karygiannis, A., Antonakakis, E., *mLab: A Mobile Ad Hoc Network Test Bed*, 1st International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing

Over the last few years, research in the area of mobile ad hoc networks (MANETs) has focused on routing protocol performance improvements, security enhancements, power consumption optimizations, and quality of service metrics. The availability of sophisticated network simulation tools, such a NS2 and GloMoSim, has allowed researchers to study MANETs without purchasing the mobile nodes themselves or conducting costly and time-consuming field trial tests. While there is an abundance of research based on simulations, actual implementations of ad hoc routing protocols and applications are very limited by comparison. Although proposed application areas benefiting from MANETs range from sensor networks, vehicle safety, military reconnaissance, first responder assistance, smart homes, and factory automation, these application scenarios have remained largely the domain of university researchers or government funded laboratories. This paper presents a MANET test bed currently under development whose goal is to help researchers and developers bridge the gap between simulations and actual MANET deployments.

Karygiannis, A., Tsiounis, Y., Kayias, A., *A Solution for Wireless Privacy and Payments Based on E-Cash*, IEEE/CreateNet

SecureComm 2005, First IEEE CreateNet Conference on Security and Privacy for Emerging Areas in Communication Networks

With wireless capable devices becoming more and more accessible, there is an increasing need for standardization of wireless networking. One of the most utilized standards that is deployed by many current devices (including the Windows XP OS) for building wireless LANs is the IEEE 802.11. For the purpose of authentication the IEEE 802.1x standard has been proposed, a flexible and extensible standard that couples 802.11 networks with various authentication services, through the incorporation of an Extensible Authentication Protocol (EAP) authentication dialog. The existing implementations of EAP dialogs are based on standard cryptographic solutions for authentication and session key generation and do not provide any form of anonymity or privacy. Anonymity and privacy are currently of pressing interest, especially in the context of WLANs, which are simultaneously the best medium to provide privacy (there is no physical phone number or connection end-point with a predetermined owner) as well as the most threatening medium to user privacy, as they have the potential of disclosing the current location of the user, in addition to their identity. At the same time, the potential “perfect hiding” capabilities of WLANs also highlight the need to control anonymity in this environment. Furthermore, paying for wireless services is completely decoupled from the above procedures, raising additional concerns of efficiency and privacy. In this work we propose a solution for Wireless privacy as well as payments by providing a new EAP authentication dialog based on anonymous electronic cash. Our solution is based on the notion of “public-key embedding e-cash”, an e-cash variant we present and formalize. We present a concrete description of the new EAP authentication dialog in the context of IEEE 802.1x. We also present an efficient implementation of a public-key embedding e-cash scheme based on RSA blind signatures and prove its security.

Kearsley, A.J., *Projections onto Order Simplexes and Isotonic Regression*, NIST Journal of Research, to be published

Isotonic regression is the problem of fitting data to order constraints. This problem can be solved numerically in an efficient way by successive projections onto order simplex constraints. An algorithm for solving the isotonic regression using successive projections onto order simplex constraints was originally suggested and analyzed by Grotzinger and Witzgall. This algorithm has been employed repeatedly in a wide variety of applications. In this paper we briefly discuss the isotonic regression problem and its solution by the Grotzinger-Witzgall method. We demonstrate that this algorithm can be appropriately modified to run on a parallel computer with substantial speed-up. Finally we illustrate how it can be used to pre-process mass spectral data for automatic high throughput analysis.

Kelsey, J., Schneier, B., *Second Primages on n-bit Hash Functions for Much Less than 2n Work*, Proceedings of Eurocrypt 2005, Margrethepladsen 1, DK-8000 Aarhus, May 21-28, 2005, published by Springer in the Lecture Notes in Computer Science

We expand a previous result of Dean [Dea99] to provide a second preimage attack on all n-bit iterated hash functions with Damgard-Merkle strengthening and n-bit intermediate states, allowing a second preimage to be found for a 2k-message-block message with about k x 2n/2+1 + 2n-k+1 work. Using RIPE-MD160 as an example, our attack can find a second preimage for a 260 byte message in about 2106 work, rather than the previously expected 2160 work. We also provide slightly cheaper ways to find multicollisions than the method of Joux[Jou04]. Both of these results are based on expandable messages--patterns for producing messages of varying length, which all collide on the intermediate hash result immediately after processing the message. We provide an algorithm for finding expandable messages for any n-bit hash function built using the Damgard-Merkle construction, which requires only a small multiple of the work done to find a single collision in the hash function.

Knill, E.H., *Quantum Computing with Realistically Noisy Devices*, Nature 434 (2005), pp. 39-44, http://math.nist.gov/quantum/,

There are quantum algorithms that can efficiently simulate quantum physics, factor large numbers and estimate integrals. As a result, quantum computers can solve otherwise intractable computational problems. One of the main problems of experimental quantum computing is to preserve fragile quantum states in the presence of errors. It is known that if the needed elementary operations (gates) can be implemented with error probabilities below a threshold, then it is possible to efficiently quantum compute arbitrarily accurately. Here we give evidence that for independent errors, the theoretical threshold is well above 3% a significant improvement over earlier calculations. However, the resources required at such high error probabilities are excessive. Fortunately, they decrease rapidly with decreasing error probabilities. If we had quantum resources comparable to the considerable resources available in today's digital computers, we could implement non-trivial quantum algorithms at error probabilities as high as 1% per gate.

Kuhn, D.R., Walsh, T.J., Fries, S., *Security Considerations for Voice over IP Systems, Recommendations of the National Institute of Standards and Technology*, NIST SP 800-58, http://csrc.nist.gov/publications/nistpubs/index.html, January 2005

Voice over Internet Protocol (VOIP) refers to the transmission of speech across data-style networks. This form of transmission is conceptually superior to conventional circuit switched communication in many ways. However, a plethora of security issues are associated with still-evolving VOIP technology. This publication introduces VOIP, its security challenges, and potential countermeasures for VOIP vulnerabilities.

Leigh, S.D., Book Review of *Statistics for the Quality Control Chemistry Laboratory*, by Eamonn Mullins, Analytical and Bioanalytical Chemistry.

Lennon, E.B., Editor, *2004 Information Technology Laboratory (ITL) Technical Accomplishments*, NISTIR 7169, http://www.itl.nist.gov/itl-publications.html, February 2005

This report presents the achievements and highlights of NIST's Information Technology Laboratory during FY 2004. Following the Director's Foreword and the ITL overview, the report describes technical projects in ITL research areas, followed by cross-cutting focus areas, industry and international interactions, publications, conferences, and staff recognition.

Lyle, J.R., Black, P.E., *Testing BIOS Interrupt 0x13 Based Software Write Blockers*, Proceedings of E-Crime and Computer Evidence Conference (ECCE2005), Monaco, March 2005

We report observations and experience in the Computer Forensics Tool Testing (CFTT) project while developing methodologies to test interrupt 0x13 based software write block (SWB) tools. A write blocker allows access to all data on a storage device while not allowing any changes to the device. A write blocker is typically used either to protect a hard drive during preview of the drive contents prior to acquiring the contents or to protect the drive during acquisition. The basic strategy is to place a filter between application programs and the storage device to be protected. The filter intercepts commands to the hard drive and only allows those that do not change the device. Such a filter can be implemented either in software or in hardware. A software program has advantages over a hardware device, but also has disadvantages. A two-piece test harness tests the SWB. The driver piece sends commands to the SWB tool. The monitor piece intercepts and counts the commands allowed by the SWB tool. The test harness itself was validated separately. Although we wrote a few simple programs to exercise the test harness, we relied mainly on manual code reviews. The anomalies found would not cause invalid testing results. Seven software write block tools have been tested: four versions of one tool, HDL, and three versions of another, PDBLOCK. No two versions behaved in exactly the same way, partly because the philosophy of write blockers has evolved. The original design of only block known writes has given way to a only allow known reads design. The latter is safer, for instance, when a new write command is added. All tools tested blocked the same core set of write commands, but there were minor variations in other categories of commands.

Lyon, G.E., Mink, A., Van Dyck, R.E., *Toward an Architectural Framework to Improve Accountability in the Use of Electronic Records*, NISTIR 7157, http://w3.antd.nist.gov/pubs05.shtml, May 2005

Sensitive electronic record systems (ERSs) raise questions about their proper use. Insider-threat involves hidden, unknown and unanticipated activities that constitute unacceptable use of an ERS, even while operating within individual access privileges. Insider-threat detection and control is an ERS monitoring and management challenge of the first order. A flexible preliminary framework can encourage discussion and comparison among various monitoring elements for the insider-threat. Responding to a lack of such a framework, one is sketched here: It employs two perspectives of an ERS user -- structural and intentional. The structural view is short term, whereas the intentional view seeks to discover general content topics of interest to a user, and to follow these over time. Discussion includes details of a possible architecture that uses untrained classification methods to amplify the concern set beyond that specifically defined at the onset of monitoring. The general framework may expedite development of common guidelines and methodologies to monitor insider threats. Although developed for medical services (e.g., an E-Health RS), the framework likely has applicability in other similar database areas such as security and intelligence archiving.

Lyon, G.E., *The Internet Marketplace and Digital Rights Management*, Digital Rights Management: Concepts and Applications, S.S. Kambhammettu (ed.), Le Magnus University Press, Nagarjuna Hills, Hyderabad, India, January 2005, Chapter 6, pp. 103-122.

Lacking physical control over Internet receiving environments, traditional information security methods cannot fully protect digital products. Insisting upon physical control severely restricts the Web market for digital objects and stymies e-commerce. Early digital rights management (DRM) reflects this dilemma, providing only limited scopes of application and suffering from poor usability. Three views—of customers, of losses, and of applications—help clarify considerations for a less restrictive next-generation DRM. Suggestions include substituting trust for diminished physical control via (i) biometrics to ease use and tighten identity binding and (ii) third- parties to rate participants and underwrite transactions.

Marbukh, V., *Intelligent Plane as a Mapping Mechanism for User Level Performance Optimization: A Case of Reliable Services over Unreliable Network*, NISTIR 7245, http://w3.antd.nist.gov/pubs05.shtml

This paper proposes a framework for balancing competing user level requirements by resolving the corresponding trade-offs in a distributed system with limited resources. Assuming that each user's preferences can be characterized by some utility function, the goal of balancing competing requirements for each user as well as across different users is to maximize the aggregate utility. The framework assumes a presence of Intelligent Plane, which isolates users from details of the network properties and mechanisms of implementation of the user level requirements. The Intelligent Plane performs the following tasks: (a) maps the user level requirements into the network resource requirements, (b) maps the resource congestion prices into prices of the user level requirements, and (c) maps the user willingness to pay for the user level requirements into payments for the specific sets of resources. Once payments for the specific sets of resources are identified, the resources are allocated to the users by a “TCP-friendly” algorithm. The paper discusses this framework for a particular case of balancing user requirements for throughput and survivability in an unreliable network, where survivability is achieved through redundancy, e.g., using multipath routing.

Marbukh, V., Klink, S., *Towards Learning in Self-Managed Systems: Cross-Layer Optimization in TCP/IP Networks*, TBD

Developing optimized distributed protocols for large-scale, self-managed systems is a challenging problem due to scalability and stability concerns. Scalability concerns can be naturally addressed by viewing distributed protocols as a non-cooperative game of local protocol components so that individual user optimizations result in the optimal overall system performance. One of the difficulties in implementing this approach is developing adaptive algorithms capable of learning of the expected user utilities and adjusting the corresponding control actions for the purpose of approaching the solution to the corresponding game, and thus optimization of the global system performance. It is known that the best response by each component to its expected utility may result in unstable behavior and deterioration of the overall performance. On an example of cross-layer optimization of a TCP/IP network, this paper discusses the possibility of avoiding these undesirable effects by allowing the control actions occasionally deviate from their best response values. Using simulations, the paper suggests that (a) sufficient level of randomness in the route selection improves the network performance, (b) the optimal level of randomness keeps the network within the stability region in close proximity to the border of this region, and (c) it may be possible to optimize the network performance by learning and adjusting the level of randomness.

McCabe, R.M., Garris, M.D., *Summary of April 2005 ANSI/NIST Fingerprint Standard Update Workshop*, NISTIR 7242, http://fingerprint.nist.gov/standard/, July 2005

This workshop was convened to chart the future of the ANSI/NIST-ITL 1-2000 fingerprint data exchange standard. This report is intended to provide a summary of that workshop. The current and future requirements and capabilities of existing stakeholders were first examined. Developments in information technology including XML were described and their potential relationship to the standard demonstrated. Approaches were presented for harmonizing this standard with other biometric standards. Additional proposals for improving the standard were introduced and a roadmap to upgrading the current version of the standard was generated.

Mead, S.L., *The Impact of RAID on Disk Imaging*, NISTIR, to be published

The goal of the Computer Forensic Tool Testing (CFTT) project is to ensure tools used by law enforcement produce accurate and objective results. The first function addressed was disk imaging. NIST developed specifications, assertions, and testing methodology to assess how well imaging tools function.

In the time since the disk imaging specifications were developed, Redundant Arrays of Inexpensive Disks (RAID) devices are increasingly being encountered by law enforcement. This paper examines RAID, and identifies where it may impact disk imaging in either completeness or accuracy. Additionally, findings that might be of special concern to investigators were identified and researched further.

From the disk imaging perspective, RAID can be viewed in three general cases. The first case is where the RAID is constructed entirely through software. Since the drives directly accessible by the disk imaging tool, software RAID has no impact. The second case is where a hardware RAID controller is used, but the drives are physically removed and imaged separately—again this presents no difficulties for the disk imager. In the last case, where an intact hardware RAID is imaged, the disk imager is affected in completeness and accuracy.

When a RAID is imaged through the hardware controller, completeness of the image is impacted. For each drive participating in the array, space is used to help construct the array and not visible to the disk imager. Furthermore, depending on the configuration of the RAID, the various drives may only have a portion of its space available for RAID—this would be expected if different sized drives were used. In terms of accuracy, depending on the type of RAID, this can be impacted as well. In the case of RAID-1 (mirror), some controllers allow reads to take place off any drive participating in the mirrored array, mixing the imaged data between the drives.

From the investigators point of view, RAID presents some difficulties that they need to be aware of. First, due to RAID, hashes between mirrored drives may not match. Second, depending on how the controller is configured, it is possible to hide partitions that are virtually undetectable if the RAID is imaged intact. Third, great care needs to be taken in identifying the configuration of the RAID, drive placement, and RAID type, as the hardware controllers may not be compatible.

Micheals, R.J., Boult, T.E., *Is the Urn Well-Mixed? Uncovering False Cofactor Homogeneity Assumption in Evaluation*, NISTIR 7156, http://www.itl.nist.gov/iad/pubs/pubs2.html, October 2004

Measuring system performance is conceptually straightforward; it is the interpretation of the results and their use as predictors of future performance that are the exceptional challenges in system evaluation and the experimentation in general. Good experimental design is critical in evaluation, but there have been very few techniques that a scientist may use to check their design for either overlooked associations or weak assumptions. For biometric and vision system evaluation, the complexity of the systems make a thorough exploration of the problem space impossible. This lack of verifiability in experimental design is a serious issue. In this paper, we present a new evaluation methodology that aids the researcher in discovering false assumptions about the homogeneity of cofactors – when the data is not "well mixed." The new methodology is then applied in the context of a biometric system evaluation.

Michel, M., Stanford, V.M., Galibert, O., *Network Transfer of Control Data: An Application of the NIST Smart Data Flow*, Journal of Systemics, Cybernetics, and Informatics, to be published

Pervasive Computing environments range from basic mobile point of sale terminal systems, to rich Smart Spaces with many devices and sensors such as lapel microphones, audio and video sensor arrays and multiple interactive PDA acting as electronic brief cases, providing authentication, and user preference data to the environment.
These systems present new challenges in distributed human-computer interfaces such as how to best use sensor streams, distribute interfaces across multiple devices, and dynamic network management as users come an go, and as devices are added or fail.

The NIST Smart Data Flow system is a low overhead, high bandwidth transport mechanism for standardized multi-modal data streams. It is designed to allow integration of multiple sensors with distributed processing needed for the sense-recognize-respond cycle of multi modal user interfaces. Its core is a server/client architecture, allowing clients to produce or subscribe to data flows, and supporting steps toward scalable processing, distributing the computing requirements among many network connected computers and pervasive devices.

This article introduces the communication broker and provides an example of an effective real time sensor fusion to track a speaker with a video camera using data captured from multi-channel microphone array.

Mills, K., Editor, *Network for Pervasive Computing*, NIST SP 500-259, http://w3.antd.nist.gov/pubs05.shtml, July 2005

Information technology is undergoing a paradigm shift from desktop computing, where isolated workstations connect to shared servers across a network, to pervasive computing, where myriad portable, embedded, and networked information appliances continuously reconfigure themselves individually and collectively to support the information requirements of mobile workers and work teams. This shift will not occur overnight, nor will it be achieved without solving a range of new technical and social problems. Still, this inexorable change should yield many economic opportunities for the global information technology industry, and for the increasing swath of businesses that depend on information. The potential value of pervasive computing motivated the NIST Information Technology Laboratory (ITL) to establish a five-year program of research to help the information technology industry identify and solve some looming technical roadblocks that seemed likely to slow development and acceptance of the new paradigm. The ITL Pervasive Computing program addressed three general areas: human-computer interaction, programming models, and networking. This special publication provides a compendium of technical papers published by NIST researchers who investigated networking for pervasive computing.

Mills, K., Quirolgico, S., Dabrowski, C., *Understanding Failure Response in Service Discovery Systems*, Journal for Cluster Computing, to be published

Service discovery systems enable distributed components to find each other without prior arrangement, to express capabilities and needs, to aggregate into useful compositions, and to detect and adapt to changes. First-generation discovery systems can be categorized based on one of three underlying architectures and on choice of behaviors for discovery, monitoring, and recovery. This paper reports a series of investigations into the robustness of designs that underlie selected service discovery systems. The paper presents a set of experimental methods for analysis of robustness in discovery systems under increasing failure intensity. These methods yield quantitative measures for effectiveness, responsiveness, and efficiency. Using these methods, we characterize robustness of alternate service discovery architectures and discuss benefits and costs of various system configurations. Overall, we find that first-generation service discovery systems can be robust under difficult failure environments. This work contributes to better understanding of failure behavior in existing discovery systems, allowing potential users to configure deployments to obtain the best achievable robustness at the least available cost. The work also contributes to design improvements for next-generation service discovery systems.

Mills, K., Tan, C., *Performance Characterization of Decentralized Algorithms for Replica Selection in Distributed Object Systems*, Proceedings of the International Workshop on Software Performance 2005, July 11, 2005, http://w3.antd.nist.gov/pubs05.shtml

Designers of distributed software systems often rely on server replicas for increased robustness, scalability, and performance. Replicated server architectures require some technique to select a target replica for each client transaction. In this paper, we survey key concepts related to replica selection and we use simulation to characterize performance (response time, server latency, selection error, probability of server overload) for four common replica-selection algorithms (random, greedy, partitioned, weighted) when applied in a decentralized form to client queries in a distributed object system deployed on a local network. We introduce two new replica-selection algorithms (balanced and balanced-partitioned) that give improved performance over the more common algorithms. We find the weighted algorithm performs best among the common algorithms and the balanced algorithm performs best among all those we considered. Our findings should help designers of distributed object systems to make informed decisions when choosing among available replica-selection algorithms.

Mitchell, W.F., *Hamiltonian Paths through Two- and Three-Dimensional Grids*, NIST Journal of Research, Vol. 110, No. 2, March/April 2005, http://nvl.nist.gov/nvl3.cfm?doc_id=89&s_id=117

This paper addresses the existence of Hamiltonian paths and cycles in two-dimensional grids consisting of triangles or quadrilaterals, and three-dimensional grids consisting of tetrahedra or hexahedra. The paths and cycles may be constrained to pass from one element to the next through an edge, through a vertex, or be unconstrained and pass through either. It was previously known that an unconstrained Hamiltonian path exists in a triangular grid under very mild conditions, and that there are triangular grids for which there is no through-edge Hamiltonian path. In this paper we prove that a through-vertex Hamiltonian cycle exists in any triangular or tetrahedral grid under very mild conditions, and that there exist quadrilateral and hexahedral grids for which no unconstrained Hamiltonian path exists. The existence proofs are constructive, and lead to an efficient algorithm for finding a through-vertex Hamiltonian cycle.

Montavont, N., Montavont, J., Noel, T., *Enhanced Schemes for L2 Handover in IEEE 802.11 Networks and their Evaluations*, Proceedings PIMRC 2005, 16th IEEE International Symposium on Personal, Indoor & Mobile Radio Communications, Berlin, DE, September 2005

Given the relatively limited coverage area of 802.11 access points, stations moving inside WLAN are often required to perform a handover. The time needed for a STA to switch from one AP to another is too long for real-time applications to continue operating seamlessly, even if no layer 3 handover is to occur ulteriorly. Many solutions have been proposed for improving the layer 2 handover latency, but we have observed a lack of performance analysis and comparison of the different algorithms. In this article we present two new schemes that aim to enhance L2 handover mechanisms. The main characteristic of these new methods is to reduce the discovery time. We then provide an evaluation of four algorithms in order to analyze and compare solutions in six different scenarios.

Morse, E., Steves, M.P., Scholtz, J.C., *Metrics and Methodologies for Evaluating Technologies for Intelligence Analysts*, 2005 International Conference on Intelligence Analysis, to be published

In this paper we discuss the evaluation methodologies and metrics we have developed for ARDA's Novel Intelligence for Massive Data (NIMD) program. We discuss the challenges of developing methods and metrics in a situation where software components that were to be tested were in very early stages of development and where investigators who might be on the leading edge with respect to their technology were novices with respect to evaluation. Additionally, we discuss how our process of evaluation design is evolving as we gain experience with metrics and measures that are obtainable, yet have some value as indicators of future software performance in the field.

Neuman, C., Hastings, N.E., Polk, W.T., *4th Annual PKI R&D Workshop: Multiple Paths to Trust Proceedings*, NISTIR 7224, August 2005

NIST hosted the fourth annual Public Key Infrastructure (PKI) Research Workshop on April 19-21, 2005. The two and a half day event brought together PKI experts from academia, industry, and government to explore the remaining challenges in deploying public key authentication and authorization technologies. This proceedings includes the seventeen refereed papers, and captures the essence of the six panels and interaction at the workshop.

The workshop also included a work-in-progress session and a birds-of-a-feather session during the evenings at the workshop hotel. Attendees included presenters from the United Kingdom, Canada, New Zealand, and Japan. Due to the success of this event, a fifth workshop is planned for April 4-6, 2006.

Park, M. H., Hong, Y. K. Choi, B. C., Gee, S. H., Donahue, M. J., *Vortex Head-to-Head Domain Walls and Their Formation in Onion-State*, Physical Review Letters, to be published

Magnetization configuration of vortex head-to-head (HTH) domain walls and the wall formation process in Ni80Fe20 ring elements were investigated using magnetic force microscopy and micromagnetic simulation. At remanence, two types of vortex HTH domain walls were observed to be stable in the onion configuration, depending on the film thickness: single- and double-vortex HTH domain walls for 40 nm and 65 nm thick ring elements, respectively. As the vortex core nucleated during formation of the HTH domain wall, exchange energy began to decrease, accompanied by an increase in the width of the wall. Vortex nucleation in the 65 nm thick ring was found to be much faster than in the 40 nm thick ring element. This effect can be attributed to the higher initial magnetostatic energy density in the thicker ring.

Peralta, R.C., *Cryptographic Primitives Can Be Fragile*, ISO Press, NATO Science Series, to be published

We show that a well-known coin-flipping protocol is breakable in the sense that one of the parties can pre-determine the result of the coin-flip. The way in which the protocol fails is illustrative of the fact that there are insecure ways of using secure cryptographic primitives.

Phillips, P.J., Flynn, P.J., Scruggs, T., Bowyer, K.W., Chang, J., Hofman, K., Marques, J., Min, J., Worek, W., *Overview of the Face Recognition Grand Challenge*, NISTIR 7195 and IEEE Computer Society International Conference on Computer Vision and Pattern Recognition 2005

Over the last couple of years, face recognition researchers have been developing new techniques, such as recognition from three-dimensional and high resolution imagery. These developments are being fueled by advances in computer vision techniques, computer design, sensor design, and interest in fielding face recognition systems. These techniques hold the promise of reducing the error rate in face recognition systems by an order of magnitude over FRVT 2002 results. The Face Recognition Grand Challenge (FRGC) is designed to achieve this performance goal by making available to researchers a data corpus of 50,000 images and a challenge problem containing six experiments. The data consists of 3D scans and high resolution still imagery. The imagery is taken under controlled and uncontrolled conditions. This paper describes the data corpus and challenge problems, and presents baseline performance and preliminary results on natural statistics of facial imagery.

Phillips, P.J., *Privacy Operating Characteristic for Privacy Protection in Surveillance Applications*, Conference on Audio- and Video-Based Biometric Person Authentication 2005, to be published

With the mass deploy of cameras, concern has risen about protecting a person's privacy as he goes about his daily life. Many of the cameras are installed to perform surveillance tasks that do not require the identity of a person. In the context of surveillance applications, we examine the trade-off better privacy and security. The trade-off is accomplished by looking at quantitative measures of privacy and surveillance performance. To provide privacy protection we examine the effect on surveillance performance of a parametric family of privacy function.

A privacy function degrades images to make identification more difficult. By varying the parameter, different levels of privacy protection are provided. We introduce the privacy operating characteristic (POC) to quantitatively show the resulting trade-off between privacy and security. From a POC, policy makers can select the appropriate operating point for a surveillance system with regard to privacy.

Podio, F.L., *International Biometric Standards - Addressing the Customer Needs for Personal Authentication*, ISO Focus, November

2004

Authentication is the provision of assurance of the claimed identity of an entity. Biometrics is defined as the automated recognition of individuals based on their behavioral and biological characteristics. Behavioral characteristics are traits that are learned or acquired, such as dynamic signature verification and keystroke dynamics. Biological characteristics include hand and facial features, fingerprints, and iris patterns. In addition to supporting national security and preventing ID fraud, they are starting to play a crucial role in enterprise-wide network security infrastructures, the protection of buildings from unauthorized individuals, employee IDs, secure electronic banking and financial transactions, retail sales, law enforcement and health and social services. Mobile devices, colleges, and amusement parks are already benefiting from these technologies. In the last few years, national security priorities have emphasized the need for biometrics in employee identification documents, passports and other high secure applications. These activities are inherently global in scope. These needs for biometric technologies have encouraged international biometric standardization. ISO/IEC JTC 1 established Subcommittee 37 – Biometrics in June 2002 in response to these users' immediate needs, and to ensure a high priority, focused, and comprehensive approach worldwide for the rapid development and approval of biometric standards. Twenty seven member countries are involved in this endeavor. The article describes the current activities of this Subcommittee, its program of work, and the interrelationship with other standards bodies and outside organizations. It emphasizes also early adoption of international biometric standards developed under SC 37 by large organizations such as the International Civil Aviation Organization and the International Labor Organization of the UN.

Podio, F.L., *ISO/IEC JTC 1 SC 37's Response to the Global Challenges and Customer Needs for Strong Personal Authentication and Enhanced Security*, ISO Focus, to be published

Biometric technologies are able to establish or verify personal identity against previously enrolled individuals. Used alone or together with other authentication technologies such as tokens they can provide higher degrees of security than other technologies employed alone and they can also overcome their weaknesses. World events in the last few years have increased the global interest for highly secure personal authentication. National security priorities have emphasized the need for biometrics in Machine Readable Travel Documents, employee identification documents, and other secure applications. Deploying new and secure information systems in support of these new global priorities require a comprehensive set of international biometrics standards developed in a timely fashion. ISO/IEC JTC 1 SC 37 – Biometrics is responding to the global challenges and customer needs for strong personal authentication and enhanced security by developing a comprehensive portfolio of biometric standards. The article discusses the customer needs for these standards, it describes the biometric standards portfolio of SC 37 and addresses how these standards will support highly secure biometric-based applications. Adoption of a number of the standards developed by SC 37 by large international organizations such as the International Civil Aviation Organization and the International Labor Office of the United Nations is also discussed.

Polk, W.T., Dodson, D.F., Burr, W.E., *Cryptographic Algorithm s and Key Sizes for Personal Identity Verification*, NIST SP 800-78, http://csrc.nist.gov/publications/nistpubs/index.html, April 2005

The Homeland Security Presidential Directive HSPD-12 called for the creation of new standards for interoperable identity credentials for physical and logical access to Federal government locations and systems. Federal Information Processing Standard 201 (FIPS 201), Personal Identity Verification (PIV) of Federal Employees and Contractors, was developed to establish standards for identity credentials. This document, Special Publication 800-78 (SP 800-78), specifies the cryptographic algorithms and key sizes for PIV systems and is a companion document to FIPS 201.

Quirolgico, S., Assis, P., Westerinen, A., Baskey, M., Stokes, E., *Toward a Formal Common Information Model Ontology*, Ontologies for Networked Systems (ONS04), http://w3.antd.nist.gov/pubs04.shtml

Self-managing systems will be highly dependent upon information acquired from disparate applications, devices, components and subsystems. To be effectively managed, such information will need to conform to a common model. One standard that provides a common model for describing disparate computer and network information is the Common Information Model (CIM). Although CIM defines the models necessary for inferring properties about distributed systems, its specification as a semi-formal ontology limits its ability to support some important requirements of a self-managing distributed system including knowledge interoperability and aggregation, as well as reasoning. To facilitate the interoperability and aggregation of CIM-based knowledge, as well reasoning over such knowledge, there is a need to model, represent and share CIM as a formal ontology. In this paper, we propose a framework for constructing a formal CIM ontology based on previous research that identified mappings from UML to ontology language constructs.

Radack, S.M., Editor, *Biometric Technologies: Helping to Protect Information and Automated Transactions in Information Technology Systems*, ITL Bulletin, http://csrc.nist.gov/publications/nistbul/index.html, September 2005

This bulletin summarizes some of ITL's activities to support the development of biometric standards, measurements, and tests for fingerprint matching, face recognition, iris recognition and speech recognition. The bulletin provides information about ITL support for the development of voluntary industry standards and the development of conformance tests, reference implementations, and evaluation procedures to facilitate the implementation of standards in biometric products. It also summarizes recent legislation that directed NIST to work with other federal agencies to develop standards needed for the biometric authentication of applicants for U.S. visas.

Radack, S.M., Editor, *Implementation of FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors*, ITL Bulletin, http://csrc.nist.gov/publications/nistbul/index.html, August 2005

This bulletin provides information about the implementation of FIPS 201. The standard specifies the technical and operational requirements for interoperable PIV systems that issue PIV cards as identification credentials and that use the cards to authenticate an individual's identity. NIST developed Special Publication (SP) 800-79, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations, to help agencies that are preparing to issue PIV cards. The bulletin explains the processes that should be carried out to assure the reliability of the PIV card issuer (PCI). Recently developed supplementary guidelines and recommendations that support agencies in implementing the technical and administrative requirements of FIPS 201 are discussed, and information is provided about the conformance testing program started by NIST to assure that for the standard.

Radack, S.M., Editor, *NIST's Security Configuration Checklists Program for Technology Products*, ITL Bulletin, http://csrc.nist.gov/publications/nistbul/index.html, June 2005

This bulletin describes the NIST security configuration checklists program and is based on NIST Special Publication 800-70: Security Configuration Checklists Program for IT Products, by Murugiah Souppaya, John Wack and Karen Kent. The bulletin discusses checklists and their benefits, and explains how the program operate. It describes the policies, procedures, and general requirements for participation in the program, and explains how to retrieve checklists from NIST's repository.

Radack, S.M., Editor, *Personal Identity Verification (PIV) of Federal Employees and Contractors: Federal Information Processing Standard (FIPS) 201 Approved by the Secretary of Commerce*, ITL Bulletin, http://csrc.nist.gov/publications/nistbul/index.html, March 2005

Federal Information Processing Standard (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, was approved by Carlos M. Guitierrez, the U.S. Secretary of Commerce, on February 25, 2005. The standard specifies a system based on the use of smart cards, which will be issued by all federal government departments and agencies to their employees and contractors who require access to federal facilities and information systems. Homeland Security Presidential Directive (HSPD) 12, issued by President Bush on August 27, 2004, directed the development of the standard for a government-wide identification system that would enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy. NIST developed the standard, working in conjunction with private industry and with other federal agencies, including the Office of Management and Budget the Office of Science and Technology Policy, and the Departments of Defense, State, Justice and Homeland Security. FIPS 201 specifies the technical and operational requirements for interoperable PIV systems that issue smart cards as identification credentials and that use the cards to authenticate an individual's identity. Information about the standard, how it was developed, and related publications is available on NIST's web site.

Radack, S.M., Editor, *Protecting Sensitive Information That is Transmitted Across Networks: NIST Guidance for Selecting and Using Transport Layer Security Implementations*, ITL Bulletin, http://csrc.nist.gov/publications/nistbul/index.html, July 2005

This bulletin summarizes guidance and information that was published by NIST to help organizations select and implement transport level security, making effective use of Federal Information Processing Standards (FIPS) approved cryptographic algorithms and open source technology. The guide, NIST SP 800-32, Guidance for the Selection and Use of Transport Layer Security (TSL) Implementations was written by C. Michael Chernick (NIST), Charles Edington III (Booz Allen Hamilton), Matthew J. Fanto (NIST), and Rob Rosenthal (Booz Allen Hamilton). SP 800-52 advises organizations how to use authentication, confidentiality and integrity mechanisms to protect information at the transport layer.

Radack, S.M., Editor, *Recommended Security Controls for Federal Information Systems: Guidance for Selecting Cost-Effective Controls Using a Risk-Based Approach*, ITL Bulletin, http://csrc.nist.gov/publications/nistbul/index.html, May 2005

This ITL Bulletin summarizes NIST SP 800-53, Recommended Security Controls for Federal Information Systems and discusses the use of SP 800-53 within the context of federal agency information security programs. The bulletin covers SP 800-53 and Federal Information Security Management Act (FISMA) requirements, how to implement an effective information security program, using a risk-based approach to selecting controls, and a catalog of security controls.

Remley, K.A., Grosvenor, C.A., Johnk, R.T., Novotny, D.R., Hale, P.D., McKinley, M.D., Karygiannis, A., Antonakakis, E., *Electromagnetic Signatures of WLAN Cards and Network Security*, 5th IEEE International Symposium on Signal Processing and Information Technology (IEEE ISSPIT 2005)

The proliferation of wireless devices and the availability of new wireless applications and services raise new privacy and security concerns. Although network-layer anonymity protects the identities of the communication endpoints, the physical layer of many wireless communication protocols offers no such guarantee. The electromagnetic signal transmitted over an open communication medium can be monitored, captured, and analyzed in an effort to trace and identify users of wireless devices. In this paper we present preliminary results on the feasibility of identifying wireless nodes in a network by measuring distinctive electromagnetic characteristics or “signatures” of Wireless Local Area Network (WLAN) cards.

Roginsky, A.L., *Targeted Search: Reducing the Time and Cost for Searching for Objects in Multi-Server Networks*, 24th IEEE

International Performance, Computing, and Communications Conference, Phoenix, Arizona, April 7-9, 2005

In many applications – including P2P file sharing, content distribution networks, and grid computing – a single object will be searched for in multiple servers. In this paper, we find the provably optimal search method for such applications and develop analytical models for search time and cost. A client node searching for objects maintains statistics on where (in which servers) it has previously found objects. Using these statistics to target future searches to “popular” servers is provably optimal. For object location and request distributions that are non-uniform, which has been shown to be the case in P2P file sharing networks, this method of targeted searching is found to be more cost-effective (i.e., use less server resources) than broadcast-based searching. Our targeted search method is implemented in a prototype Gnutella servent called Ditella. Ditella can improve the scalability of file sharing in P2P networks and reduce the amount of traffic in the Internet by reducing file search query traffic.

Ross, R., Katzke, S., Johnson, A., Swanson, M., Stoneburner, G., Rogers, G., Lee, A., *Recommended Security Controls for Federal Information Systems*, NIST SP 800-53, http://csrc.nist.gov/publications/nistpubs/index.html, February 2005

The purpose of this publication is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines have been developed to help achieve more secure information systems within the federal government by: (i) facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems; (ii) providing a recommendation for minimum security controls for information systems categorized in accordance with Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems; (iii) promoting a dynamic, extensible catalog of security controls for information systems to meet the demands of changing requirements and technologies; and (iv) creating a foundation for the development of assessment methods and procedures for determining security control effectiveness. The guidelines provided in this special publication are applicable to all federal information systems other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542. The guidelines have been broadly developed from a technical perspective to complement similar guidelines for national security systems. This publication is intended to provide guidance to federal agencies until the publication of FIPS 200, Minimum Security Controls for Federal Information Systems (projected for publication December 2005).

Ross, R., Katzke, S., Toth, P., *The New FISMA Standards and Guidelines: Changing the Dynamic of Information Security for the Federal Government*, MILCOM 2005, Atlantic City, New Jersey, October 17-20, 2005

The Federal Information Security Management Act (FISMA) of 2002 places significant requirements on federal agencies for the protection of information and information systems; and places significant requirements on the National Institute of Standards and Technology (NIST) to assist federal agencies to comply with FISMA. In response to this important legislation, NIST is leading the development of key information system security standards and guidelines as part of its FISMA Implementation Project (http://csrc.nist.gov/sec-cert/index.html). This high-priority project includes the development of security categorization standards; standards and guidelines for the specification, selection, and testing of security controls for information systems; guidelines for the certification review and accreditation of information systems; and guidelines for the continuous monitoring of controls to ensure that they continue to operate as intended. This paper includes a discussion of NIST’s FISMA risk management framework (RMF) and the suite of related standards and guidelines being developed by NIST to help federal agencies comply with FISMA requirements (i.e., the FISMA suite of documents). In addition, the paper discusses how agency systems will benefit from applying the FISMA RMF, and why the FISMA RMF and the related suite of standards and guidelines should be of interest to other government sectors (e.g., DoD) and to the commercial sector.

Ross, R.S., Toth, P.R., *Understanding the NIST Standards and Guidelines Required by FISMA: How Three Mandated Documents are Changing the Dynamic of Information Security for the Federal Government*, ITL Bulletin, http://csrc.nist.gov/publications/nistbul/index.html, November 2004

This ITL Bulletin summarizes an article entitled, "Understanding the New FISMA Required NIST Standards and Guidelines," by Ron S. Ross, PhD.

Rouil, R., Chevrollier, N., Golmie, N., *Unsupervised Anomaly Detection System Using Next-Generation Router Architecture*, MILCOM 2005, Atlantic City, New Jersey, October 17-20, 2005, http://w3.antd.nist.gov/pubs05.shtml

Unlike many intrusion detection systems that rely mostly on labeled training data, we propose a novel technique for anomaly detection based on unsupervised learning and we apply it to counter denial-of-service attacks. Initial simulation results suggest that significant improvements can be obtained. We then discuss an implementation of our anomaly detection system in the ForCES router architecture and evaluate it using attack traffic.

Rukhin, A.L., *Conservative Confidence Intervals Based on Weighted Means Statistics*, Statistics and Probability Letters, to be published

For weighted means estimators of the common mean of several normal populations associated (conservative) confidence intervals are constructed. These intervals are compared to several traditional confidence bounds. Monte Carlo simulation results of these comparisons are reported.

Rukhin, A.L., *Nonparametric Inference for Balanced Randomization Designs*, Journal of Statistical Planning and Inference, to be published

The properties of two balanced randomization schemes which allocate the known number of subjects among several treatments are compared. According to the first procedure, the so-called truncated multinomial randomization design, the allocation process starts with the uniform distribution, until a treatment receives the prescribed number of subjects, after which this uniform distribution switches to the remaining treatments, and so on. The second scheme, the random allocation rule, selects at random any assignment of the given number of subjects per treatment. The limiting behavior of these two procedures is shown to be quite different in the sense that for the random allocation rule the instant, at which a treatment gets its prescribed number of subjects, comes much later. The large sample distribution of standard permutation tests is obtained, and formulas for the accidental bias and for the selection bias of both procedures are derived.

Rukhin, A.L., Pattern Correlation Matrices for Markov Sequences and Tests of Randomness, Probability Theory and its Applications, to be published

The paper derives some properties of the so-called pattern correlation matrices which are useful in statistical analysis of random Markov sequences. Asymptotic expansions for the probability that a given word occurs in the string a given number times and of joint occurrences for two words are derived. The covariance matrix of the joint distribution of frequencies of all patterns is expressed in terms of the pattern correlation matrix, and a simple generalized inverse of this covariance matrix is given. Relevant statistical implications for goodness-of-fit testing are formulated.

Rukhin, A.L., Recognition Problem of Biometrics: Nonparametric Dependence Measures and Aggregated Algorithms, Statistical Methods in Counter-Terrorism, to be published

Biometric systems designed to detect or verify a person's identity are widely used in homeland security. A variety of commercially available biometric systems are now in existence; current technological progress makes it possible to evaluate these systems consistently and comprehensively. Recognition or identification problem of biometrics is important for such evaluations.
In identification systems, a biometric signature of an unknown person, a probe, is presented to a system, which compares the new signature with a database of biometric signatures of known individuals. On the basis of this comparison, the system reports the similarity scores of the probe to the signatures in this database, called the gallery. The gallery items are then ranked accordingly to their similarity scores of the probe; the top matches with highest similarity scores are expected to contain the true identity.
This work addresses two following issues: how to compare algorithms on the basis of their similarity scores for face recognition and how to combine different algorithms. An example from the FERET (Face Recognition Technology) program with four face recognition algorithms is examined.

Rust, B.W., Donnelly, D., *The Fast Fourier Transform for Experimentalists Part IV: Autoregressive Spectral Analysis*, Computing in Science and Engineering, to be published

This tutorial paper is the fourth in a series devoted to the use of the Fast Fourier Transform (FFT) in time series analysis. It describes the parametric methods for estimating the power spectral density (PSD) that are used when the time series is assumed to be well modeled by an autoregressive process. In such cases, the PSD estimates can be calculated from estimates of the autoregressive parameters. A special case is the Maximum Entropy Method (MEM) which seeks the parameter estimates which minimize the assumptions about the data outside the window of observation. In all of these methods, the results are strongly dependent on the choice of the order of the autoregressive process. Two simple noisy time series are use to illustrate these issues.

Rust, B.W., *Carbon Dioxide, Global Warming, and Michael Crichton's "State of Fear,"* Computing Science and Statistics, to be published

In his recent novel, State of Fear (HarperCollins, 2004), Michael Crichton questioned the connection between global warming and increasing atmospheric carbon dioxide by pointing out that for 1940-1970, temperatures were decreasing while atmospheric carbon dioxide was increasing. A reason for this contradiction was given at Interface 2003 [B.W. Rust, Computing Science and Statistics, 35 (2003) 263-277] where the temperature time series was well modeled by a 64.9 year cycle superposed on an accelerating baseline. For 1940-1970, the cycle decreased more rapidly than the baseline increased. We will soon enter another cyclic decline, but the temperature hiatus this time will be less dramatic because the baseline has accelerated. This paper demonstrates the connections between fossil fuel emissions, atmospheric carbon dioxide concentrations, and global temperatures by simultaneously modeling their measured time series.

Saunders, B., Wang, Q., *Boundary/Contour Fitted Grid Generation for Effective Visualizations in a Digital Library of Mathematical Functions*, NISTIR 7228 and Proceedings of the 9th International Conference on Numerical Grid Generation in Computational Field Simulations, to be published

Effective visualizations can help researchers obtain a more complete understanding of high-level mathematical functions that arise in mathematics, statistics, physics, fluid dynamics and other fields of the mathematical and physical sciences. Accordingly, dynamic interactive 3D graphs of function surfaces will be a key feature of the NIST digital Library of Mathematical Functions, a new Web-based compendium of mathematical functions that will replace a popular but dated resource, the National Bureau of Standards

Handbook of Mathematical functions, published by Abramowitz and Stegun in 1964. As developers of commercial packages are well aware, creating software to accurately plot complicated 3D surfaces can be a challenging task. This paper looks at the effectiveness of modifying an algebraic tensor product spline grid generation technique, whose design was originally motivated by problems in aerodynamics and solidification theory, to create computational grids for accurate visualizations of 3D surfaces that capture key function features such as poles, branch cuts, and other singularities.

Sayrafian-Pour, K., Kaspar, D., *Indoor Positioning Using Spatial Power Spectrum*, 16th Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications, September 11–14, 2005

A simple technique to estimate the position of a given mobile source inside a building is based on the received signal strength. For this methodology to have a reasonable accuracy, radio visibility of the mobile by at least three access points is required. To reduce the number of the required access points and therefore simplify the underlying coverage design problem, we propose a new scheme that takes into account the distribution of RF energy around the receiver. In other words, we assume that the receiver is equipped with a circular antenna with beamforming capability. In this way, the spatial spectrum of the received power can be measured by rotating the antenna beam around the 360-degree field of view. This spatial spectrum can be used by a single receiver as a mean for estimating the position of a mobile transmitter. In this paper, we investigate the feasibility of this methodology, and show the improvement achieved in the positioning accuracy.

Scholtz, J., Theofanos, M.F., Consolvo, S., *A Framework for the Evaluation of Pervasive Information Systems*, Book chapter in Pervasive Information Systems, to be published

In this chapter we present a framework of areas of evaluation for pervasive information systems along with metrics and examples from the literature. We review a number of methodologies that have been used in evaluation. A case study of an evaluation using a number of the evaluation areas in the framework is also given. We conclude with a discussion of future needs to enable researchers to share evaluation results.

Scholtz, J.C., Antonishek, B., Young, J., *A Field Study of Two Techniques for Situation Awareness for Robot Navigation in Urban Search and Rescue*, IEEE Ro-Man 2005 Conference, August 13-15, 2005, accepted for publication

In this paper we examine the performance of robot systems that use two different techniques for situation awareness for operators of robots in an urban search and rescue (USAR) competition: an automatic mapping technique using sonar and laser sensors and the use of an overhead camera to provide a frame of reference. In order to analyze situation awareness, we classified a subset of critical incidents that occurred during the RoboCup 2004 competition. While we conclude that both techniques lower critical incidents in local navigation and obstacle encounters, this result should be interpreted with caution as it is based on our field study results. A more controlled laboratory follow up study is planned.

Scholtz, J.C., Antonishek, B., Young, J., Implementation of a Situation Awareness Assessment Tool for Evaluation of Human Robot Interfaces, IEEE Transactions on System, Man, and Cybernetics, Part A, to be published

In this paper we outline a methodology for evaluating the situation awareness (SA) provided by a supervisory interface for an autonomous on-road vehicle. Our goal is to be able to use the evaluations to compare interface designs with respect to how well each facilitates the users' acquisition of situation awareness. We used Endsely's Situation Awareness Global Assessment Technique (SAGAT) [8] and developed scenarios and assessment questions appropriate for supervisors of autonomous on-road driving vehicles. We describe the results of two experiments used to refine our SA assessment implementation. In a third experiment we applied the refined implementation to a graphical user interface we developed to test the sensitivity of our SAGAT implementation. We discuss the results of this experiment and implications for applying the SAGAT methodology to supervisory user interfaces for autonomous vehicles.

Scholtz, J.C., Antonishek, B., Young, J.D., *Evaluation of Human-Robot Interaction in the NIST Reference Search and Rescue Test Arenas*, Performance Metrics for Intelligent Systems 2004 Workshop Proceedings, PerMIS '04, August 24, 2004, http://www.itl.nist.gov/iad/IADpapers/2004/Scholtz_PerMIS_2004.pdf

We describe data collections that we have conducted during Urban Search and Rescue (USAR) competitions within the NIST Reference Test Arenas. We also discuss our analyses of this data and present guidelines based on these studies. We also describe future plans for augmenting USAR competitions to specifically compare different methods of human-robot interaction (HRI).

Scholtz, J.C., *Metrics for Evaluation of Software Technology to Support Intelligence Analysis*, Human Factors and Ergonomics Society 2005, to be published

For the past two years we have been involved in evaluation of software technologies designed to improve analysis. We have been conducting evaluations both in the laboratory and in operational environments. While usability is an important aspect of software for intelligence analysis, our work has gone beyond usability and focused on utility. We have been using top-down and bottom –up procedures to develop metrics and evaluation methodologies, including literature reviews and expert opinions, laboratory studies, baseline creation, and field observations. Our laboratory work has focused on strategic, open source analysis. Our field work to date has been more in the tactical area all source domain. In this paper, we discuss a number of metrics we have developed and outline some issues involved in evaluation of software to support intelligence analysts.

Scholtz, J.C., Morse, E., Hewett, T.T., *An Analysis of Qualitative and Quantitative Data from Professional Intelligence Analysts*, 2005 International Conference on Intelligence Analysis, to be published

Our goal is to produce metrics for measuring the effectiveness of software tools and environments produced for the intelligence community. To this end we need to understand the analytic process and to determine which data need to be captured to meaningfully measure process and effectiveness. In this paper we compare data from observational studies of professional intelligence analysts with data collected from an instrumented environment. We discuss some findings and their implications for possible metrics and for additional data needed to compute potential measures.

Scholtz, J.C., *The Effect of Situation Awareness Acquisition in Determining the Ratio of Operators to Semi-Autonomous Driving Vehicles*, The International Society for Optical Engineering, http://www.itl.nist.gov/iad/pubs/pubs2.html

We used a technical readiness level assessment to obtain intervention time and the time to acquire situation awareness for different classifications of interventions. We analyzed this data to determine if it is feasible for one operator to control multiple robots of this type in similar environments. We conclude that in both terrains analyzed (an arid terrain and a wooded terrain) it would be feasible for one operator to control two robots. While it is also possible for an operator to work on another task and control a robot as well, there is an issue of providing situation awareness about the robot. There are also constraints on the tasks that could be effectively accomplished.

Sims, J.S., Hagstrom, S.A., *High Precision Variational Calculations for the Born-Oppenheimer Energies of the Ground State of the Hydrogen Molecule*, Journal of Chemical Physics, to be published

Born-Oppenheimer approximation Hylleraas (Hy) variational calculations with up to 7034 expansion terms are reported for the singlet sigma g+ ground state of neutral hydrogen at various internuclear distances. The nonrelativistic energy is calculated to be -1.1744 7571 4220(1) hartree at R = 1.4 bohr, which is 4 orders of magnitude better than the best previous Hylleraas calculation, that of Wolniewicz. This result agrees well with the best previous variational energy, -1.1744 7571 4216 hartree, of Cencek, obtained using Explicitly Correlated Gaussians (ECG). The uncertainty in our result is also discussed. The nonrelativistic energy is calculated to be -1.1744 7593 1399(1) hartree at the equilibrium R = 1.4011 bohr distance. This result also agrees well with the best previous variational energy, -1.1744 7593 1389 hartree, of Cencek and Rychewski\cite {Ry:03,Ry:03a}, obtained using Explicitly Correlated Gaussians (ECG).

Slattery, O.T., *Drive Compatibility Test (Phase 2) for DVD-R (General) and DVD+R Discs, Including DVD Creation Plan*, NIST SP 500-258, http://www.itl.nist.gov/div895/docs/NIST-SP500-258.pdf, September 2004

Phase 2 test procedure is designed to test the compatibility of DVD drives with DVD writable media including DVD-R (for general) and DVD+R. The test plan includes detailed instructions on how to create and test the recordable media and how to determine the result from each test. Following implementation of Phase 1 (NIST Special Publication 500-254), the National Institute of Standards and Technology (NIST), the Optical Technology Storage Association (OSTA) and the DVD Association (DVDA) expanded the scope of testing in Phase 2. Phase 2 includes testing of DVD recordable drives and also includes a procedure to create test media.

Slutsker, J., Thornton, K., Roytburd, A.L., Warren, A., McFadden, G.B., Voorhees, P.W., *Phase-Field Modeling of Solidification under Stress,* Acta Materialia, to be published

A phase-field model that includes the stress field during non-isothermal phase transformation of a single-component system has been developed. The model has been applied to the solidification and melting of confined spherical volumes, where sharp interface solutions can be obtained and compared with the results of the phase-field simulations. Numerical solutions for a spherically-symmetric geometry have been obtained. The analysis of these equilibrium states for the phase-field model allows us to estimate the value of interface energy in the model, which can then be compared to the analogous calculation of the energy of planar liquid-solid interface. It is also demonstrated that the modeling of the liquid as a coherent solid with zero shear modulus is realistic by comparison of the long-range stress fields in phase-field calculations with those calculated using sharp interface models of either a coherent or relaxed liquid-solid interface. The model can be applied to simulate the process of “writing” to electronic media that exploits an amorphous-to-crystalline phase change for recording information.

Soboroff, I.M., Harman, D.K., *Novelty Detection: The TREC Experience*, Proceedings of the 2005 Conference on Human Language Technology (HLT 2005)

A challenge for search systems is to detect not only when an item is relevant to the user's information need, but also when it contains something new which the user has not seen before. In the TREC novelty track, the task was to highlight sentences containing relevant and new information in a short, topical document stream. This is analogous to highlighting key parts of a document for another person to read, and this kind of output can be useful as input to a summarization system. Search topics involved both news events and reported opinions on hot-button subjects. When people performed this task, they tended to select small blocks of consecutive sentences as relevant, whereas current systems identified many relevant and novel passages. We also found that opinions are much harder to track than events.

Soboroff, I.M., *Overview of the TREC 2004 Novelty Track*, Included in NIST SP 500-261, http://trec.nist.gov/pubs.html, August 2005

TREC 2004 marks the third and final year for the Novelty Track. The task is as follows: Given a TREC topic and an ordered list of documents, systems must find relevant and novel sentences that should be returned to the user from this set. This task integrates aspects of passage retrieval and information filtering. As in 2003, there were two categories of topics-events and opinions and four subtasks which provided systems with varying amounts of relevance or novelty information as training data. This year, the task was made harder by the inclusion of some number of irrelevant documents in document sets. Fourteen groups participated in the track this year.

Somma, R., Barnum, H., Knill, E.H., Ortiz, G., Viola, L., *Generalized Entanglement and Quantum Phase Transitions*, International Journal of Modern Physics B, to be published

Quantum phase transitions in matter are characterized by structural changes in some correlation functions of the system, thus ultimately entanglement. In this work, we study the second order quantum phase transitions present in models of relevance to condensed-matter physics by exploiting the notion of generalized entanglement [Barnum et al., Phys. Rev. A 68, 032308 (2003)]. In particular, we focus on the illustrative case of a one-dimensional Ising model in the presence of a transverse magnetic field. Our approach leads to useful tools for distinguishing between the ordered and disordered phases in the case of broken symmetry quantum phase transitions. Possible extensions to the study of other kinds of phase transitions as well as of the inherent relation between generalized entanglement and computational efficiency are also discussed.

Souppaya, M., Wack, J., Kent, K., *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*, NIST SP 800-70, http://csrc.nist.gov/checklists/download_sp800-70.html, May 2005

The National Institute of Standards and Technology (NIST) has produced Security Configuration Checklists Program for IT Products: Guidance for Checklist Users and Developers to facilitate the development and dissemination of security configuration checklists so that organizations and individual users can better secure their IT products. A security configuration checklist (sometimes called a lockdown or hardening guide or benchmark) is in its simplest form a series of instructions for configuring a product to a particular security level (or baseline). It could also include templates or automated scripts and other procedures. Typically, checklists are created by IT vendors for their own products; however, checklists are also created by other organizations such as consortia, academia, and government agencies. The use of well-written, standardized checklists can markedly reduce the vulnerability exposure of IT products. Checklists may be particularly helpful to small organizations and individuals that have limited resources for securing their systems. This publication is intended for users and developers of IT product security configuration checklists. For checklist users, this document gives an overview of the NIST Checklist Program, explains how to retrieve checklists from NIST's repository, and provides general information about threat discussions and baseline technical security practices for associated operational environments. For checklist developers, the document sets forth the policies, procedures, and general requirements for participation in the NIST Checklist Program.

Souryal, M.R., Larsson, E.G., Peric, B.M., Vojcic, B.R., *Soft Decision Metrics for Turbo-Coded FH M-FSK Ad Hoc Packet Radio Networks*, 2005 IEEE Vehicular Technology Conference (VTC 2005/Spring), May 30, 2005

This paper addresses turbo-coded non-coherent FH M-FSK ad hoc networks with a Poisson distribution of interferers where multiple access interference can be modeled as symmetric α-stable (SαS) noise and α is inversely proportional to the path loss exponent. The Bayesian Gaussian metric does not perform well in non-Gaussian (α≠2) noise environments and therefore an optimum metric for Cauchy (α=1) noise and a generalized likelihood ratio (GLR) Gaussian metric requiring less side information (amplitude, dispersion) are presented. The robustness of the metrics is evaluated in different SαS noise environments and for mismatched values of the interference dispersion and channel amplitude in an interference-dominated network with no fading or independent Rayleigh fading. Both the Cauchy and GLR Gaussian metric exhibit significant performance gain over the Bayesian Gaussian metric, while the GLR Gaussian metric does so without the knowledge of the dispersion or amplitude. The Cauchy metric is more sensitive to the knowledge of the amplitude than the dispersion, but generally maintains better performance than the GLR Gaussian metric for a wide range of mismatched values of these parameters. Additionally, in an environment consisting of non-negligible Gaussian thermal noise along with multiple access interference, increasing the thermal noise level degrades the performance of the GLR Gaussian and Cauchy metric while for the observed levels both maintain better performance than the Bayesian Gaussian metric.

Souryal, M.R., Larsson, E.G., Peric, B.M., Vojcic, B.R., *Soft-Decision Metrics for Coded Orthogonal Signaling in Symmetric Alpha-Stable Noise*, Proceedings of the 2005 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), March 18, 2004

This paper derives new soft decision metrics for coded orthogonal signaling in symmetric a-stable noise, which has been used to model impulsive noise. In addition to the optimum metrics for Gaussian (a = 2) noise and Cauchy (a = 1) noise, a class of generalized likelihood ratio (GLR) metrics with lower side information requirements is derived. Through numerical results for a turbo code example, the Cauchy decoder is found to be robust for a wide range of a, and GLR metrics are found which provide performance gains relative to the Gaussian metric, but with lower complexity and less a priori information.

Souryal, M.R., Moayeri, N., *Channel-Adaptive Relaying in Mobile Ad Hoc Networks with Fading*, Proceedings of the IEEE Conference on Sensor and Ad Hoc Communications and Networks (SECON), September 26-29, 2005

This paper describes an approach for relaying in multihop networks that adapts to the time-varying channel and exploits spatial diversity to mitigate multipath fading. Ignored in some simulation-based performance analyses, fading arises from multipath propagation and causes fluctuations in the signal strength in mobile networks, adversely affecting communication performance. Our approach uses limited cross-layer interactions between the physical, link and routing layers to provide adaptivity to both large and small-scale channel effects and to achieve spatial diversity gain without the use of multiple antennas. The routing layer uses long-term measurements of link quality in the form of the average signal-to-noise ratio (SNR) to opportunistically select next-hop relays on a hop-by-hop basis. Small-scale variations are overcome at the MAC layer through efficient multicast polling of multiple next-hop candidate relays prior to data transmission. A performance analysis for networks employing geographic routing and an IEEE 802.11-based MAC (i) demonstrates significant improvements in network capacity and end-to-end delay achieved with these channel-adaptive techniques in Rayleigh and Ricean fading environments, (ii) shows that most of the small-scale diversity gain is obtained through the use of only two next-hop relay choices, and (iii) assesses the practical limit of the short-term adaptive component in terms of maximum node velocity.

Sriram, K., Montgomery, D., Borchert, O., Kim, O., Kuhn, R., *Autonomous System (AS) Isolation under Randomized BGP Session Attacks with RFD Exploitation*, International Conference on Computer Communications, IEEE INFOCOM 2006, Barcelona, Spain, April

23-29, 2006

BGP peering session attacks are known to drive routes into route flap damping (RFD) suppression states and thus cause isolations between autonomous systems (ASes) and destinations. We present a detailed study of the impact of BGP peering session attacks and the resulting exploitation of RFD that cause network-wide routing disruptions. Analytical results provide insights into the nature of the problem and impact of the attacks. Detailed simulation results using SSFNet BGP framework complement the analytical results and provide many useful insights.

Stanford, V., Rochet, C., Michel, M., Garofolo, J., *Beyond Close Talk - Issues in Distant Speech Acquisition, Conditioning Classification, and Recognition*, Included in NIST SP 500-257, Proceedings of the ICASSP 2004 Meeting Recognition Workshop, http://www.itl.nist.gov/iad/IADpapers/2004/ICASSP2004Workshop.pdf, October 14, 2004

Properly designed reference data and performance metrics can offer crucial aid to developers of advanced statistical recognition technologies. We focus here on audio data acquisition from close-talk, near field, and far field sensors, and upon its processing, and its metrology. Our intention is to support the research community as it develops state of the art data acquisition and multimodal processing algorithms by supplying standard reference data, metrics, and sharable infrastructure.

Tabassi, E., Wilson, C.L., *A Novel Approach to Fingerprint Image Quality*, ICIP 2005, The International Conference on Image Processing

We present a novel measure of fingerprint image quality, which can be used to estimate fingerprint match performance. This means presenting the matcher with good quality fingerprint images will result in high matcher performance, and vice versa, the matcher will perform poorly for poor quality fingerprints. We discuss the implementation of our fingerprint image quality metric and we present the results of testing it on 280 different combinations of fingerprint image data and fingerprint matcher system. We found that the metric predicts matcher performance for all systems and datasets. Our definition of quality can be applied to other biometric modalities and upon proper feature extraction can be used to assess quality of any mode of biometric samples.

Tang, X., Ma, L., Mink, A., Nakassis, A., Hershman, B., Bienfang, J., Boisvert, R., Clark, C., Williams, C., Gross, A., Hagley, E., Wen, J., *High Speed Fiber-Based Quantum Key Distribution using Polarization Encoding*, Proceedings of SPIE, Vol. 5893, August 2005, http://math.nist.gov/quantum/

We have implemented a quantum key distribution (QKD) system with polarization encoding at 850 nm over 1 km of optical fiber. The high-speed management of the bit-stream, generation of random numbers and processing of the sifting algorithm are all handled by a pair of custom data handling circuit boards. As a complete system using a clock rate of 1.25 Gbit/s, it produces sifted keys at a rate of 1.1 Mb/s with an error rate lower than 1.3% while operating at a transmission rate of 312.5 Mbit/s and a mean photon number μ = 0.1. With a number of proposed improvements this system has a potential for a higher key rate without an elevated error rate.

Theofanos, M.F., Scholtz, J., *A Diner's Guide to Evaluating a Framework for Ubiquitous Computing Applications*, Human Computer Interaction International Conference 2005, July 27, 2005

There is a clear need for evaluation methodologies specifically suited to ubiquitous computing applications. Here we investigate a user evaluation framework we proposed earlier which draws upon traditional desktop methods, but carefully adapts them based on our experiences with ubiquitous architectures. We test and clarify the criteria in our methodology by examining the utility and applicability of the framework to an existing commercial ubiquitous application for restaurant ordering at the tableside. We analyzed its functionality by discussing design principles with its software developers, and interviewed wait staff as well as restaurant managers to understand its impacts on the workflow and business processes. We conclude that the proposed framework does contain appropriate metrics to assess whether good design principles were achieved and if the designed system will produce the desired user experience.

Toman, B., *Linear Statistical Models with Type B Uncertainty: A Bayesian View of Annex H.3 and H.5 of the Guide to the Expression of Uncertainty in Measurement*, Metrologia, to be published

Annex H.3 of the Guide to the Expression of Uncertainty in Measurement presents an example of calibration of a thermometer using a linear regression model. Annex H.5 of the same publication presents a class of statistical models and analysis techniques which are commonly called the Analysis of Variance (ANOVA). These models are useful for accounting for the effects of factors which cause the measurand in an experiment to change over time or over experimental conditions. Both Annex H.3 and H.5 present procedures which assume that the observations are not subject to type B uncertainties. A natural question then is: Can these models be used in the presence of type B uncertainties? This article answers the question in the affirmative and provides a natural interpretation of the results. The example data from the two Annexes are used for an illustration.

Ulery, B., Hicklin, A., Watson, C., Indovina, M., Kwong, K., *Slap Fingerprint Segmentation Evaluation 2004 Analysis Report*, NISTIR 7209, http://fingerprint.nist.gov/slapseg04/index.html, March 2005

The Slap Fingerprint Segmentation Evaluation 2004 (Slap Seg04) was conducted to assess the accuracy of algorithms used to segment slap fingerprint images into individual fingerprint images. Segmenters from ten different organizations were evaluated on data from seven government sources, according to several distinct measures of accuracy. The source of data, the segmentation software used, and the decision criteria used were each found to have a significant impact on accuracy. Depending on the data source, the best segmenters produced at least 3 matchable fingers, with finger positions correctly identified, from 93% to over 99% of the slaps. The source of data is a much better predictor of success than whether the images were collected on livescan devices or paper. Most segmenters performed well, but there were significant differences among segmenters on poor quality data.

Voorhees, E.M., *Overview of the TREC 2004 Question Answering Track*, Included in NIST SP 500-261, http://trec.nist.gov/pubs.html, August 2005

The TREC 2004 Question Answering track contained a single task in which question series were used to define a set of targets. Each series contained factoid and list questions and related to a single target. The final question in the series was an "Other" question that asked for additional information about the target that was not covered by previous questions in the series. Each question type was evaluated separately with the final score a weighted average of the different component scores. Applying the combined measure on a per-series basis produces a QA task evaluation that more closely mimics classic document retrieval evaluation.

Voorhees, E.M., *Overview of the TREC 2004 Robust Retrieval Track*, Included in NIST SP 500-261, http://trec.nist.gov/pubs.html, August 2005

The robust retrieval track explores methods for improving the consistency of retrieval technology by focusing on poorly performing topics. The retrieval task in the track is a traditional ad hoc retrieval task where the evaluation methodology emphasizes a system's least effective topics. The most promising approach to improving poorly performing topics is exploiting text collections other than the target collection such as the web.

The 2004 edition of the track used 250 topics and required systems to rank the topics by predicted difficulty. The 250 topics within the test set allowed the stability of evaluation measures that emphasize poorly performing topics to be investigated. A new measure, a variant of the traditional MAP measure that uses a geometric mean rather than an arithmetic mean to average individual topic results, shows promise of giving appropriate emphasis to poorly performing topics while being more stable at equal topic set sizes.

Voorhees, E.M., *Overview of TREC 2004*, Included in NIST SP 500-261, http://trec.nist.gov/pubs.html, August 2005, to be published

This report provides an overview of the thirteenth Text REtrieval Conference, TREC 2004. TREC 2004 was held at the National Institute of Standards and Technology (NIST) November 16-19, 2004. The conference was co-sponsored by NIST, the U.S. Department of Defense Advanced Research and Development Activity (ARDA), and the Defense Advanced Research Projects Agency (DARPA). The conference attracted 103 participating groups, including academic, commercial, and government participants From 21 different countries.

Voorhees, E.M., *Using Question Series to Evaluate Question Answering System Effectiveness*, 2005 HLT Conference Proceedings

The original motivation for using question series in the TREC2004 question answering track was the desire to model aspects of dialogue processing in an evaluation task that included different question types. The structure introduced by the series also proved to have an important additional benefit: the series is at an appropriate level of granularity for aggregating scores for an effective evaluation. The series is small enough to be meaningful at the task level since it represents a single user interaction, yet it is large enough to avoid the highly skewed score distributions exhibited by single questions. An analysis of the reliability of the per-series evaluation shows the evaluation is stable for differences in scores seen in the track.

Walsh, T.J., Kuhn, D.R., *Securing Voice over Internet Protocol Networks*, ITL Bulletin, http://csrc.nist.gov/publications/nistbul/index.html, October 2004

Voice over IP – the transmission of voice over traditional packet-switched IP networks – is one of the hottest trends in telecommunications. As with any new technology, VOIP introduces both opportunities and problems. Lower cost and greater flexibility are among the promises of VOIP for the enterprise, but security administrators will face significant challenges. Administrators may assume that since digitized voice travels in packets, they can simply plug VOIP components into their already-secured networks. Unfortunately, many of the tools used to safeguard today's computer networks, namely firewalls, Network Address Translation (NAT), and encryption, carry a hefty price when incorporated into a VOIP network. This paper introduces the security issues with VOIP and outlines steps that can be taken to operate a VOIP system securely.

Walsh, T.J., Kuhn, R.D., *Securing Voice over IP Networks*, IEEE Computer Security and Privacy, to be published

Voice over IP – the transmission of voice over traditional packet-switched IP networks – is one of the hottest trends in telecommunications. As with any new technology, VOIP introduces both opportunities and problems. Lower cost and greater flexibility are among the promises of VOIP for the enterprise, but security administrators will face significant challenges. Administrators may assume that since digitized voice travels in packets, they can simply plug VOIP components into their already-secured networks. Unfortunately, many of the tools used to safeguard today's computer networks, namely firewalls, Network Address Translation (NAT), and encryption, carry a hefty price when incorporated into a VOIP network. This paper introduces the security issues with VOIP and outlines steps that can be taken to operate a VOIP system securely.

Wang, C.M., Iyer, H.K., *Detection of Influential Observation in the Determination of the Weighted-Mean KCRV*, Metrologia, to be published

Since the signing of the Mutual Recognition Arrangement, National Metrology Institutes (NMI) have carried out many key comparisons in a wide range of metrological areas to establish the equivalence of their measurement standards. The determination of a key comparison reference value (KCRV) and its associated uncertainty are the central tasks in the evaluation of key comparison data. One of the most popular ways to estimate the KCRV is to use a weighted mean of each NMI's reporting values, with weights inversely proportional to the variances of the NMI's reporting value. One potential problem with the use of the weighted mean is its reliance on the weights that may vary greatly across NMIs. Consequently, some of the NMIs can be influential in the determination of the weighted-mean KCRV. Thus it is of interest to identify the influential NMIs based on some simple and well-defined criteria. In this paper, we present several easy-to-use criteria for detecting influential data in the calculation of the weighted-mean KCRV.

Wang, C.M., Iyer, H.K., *On Higher Order Corrections for Propagating Uncertainties*, Metrologia, to be published

The ISO Guide to the Expression of Uncertainty in Measurement (GUM) recommends the use of a first-order Taylor series expansion for propagating errors and uncertainties. The GUM also suggests the use of a second-order Taylor series approximation for calculating uncertainties when the first-order approximation alone is not adequate. In this paper we derive the formulas for evaluating measurement uncertainty based on a second-order Taylor series approximation. We provide a computer program that uses symbolic derivatives to calculate the second-order approximations of the uncertainty in measurement results.

Wang, C.M., Iyer, H.K., *Propagation of Uncertainties in Measurement Using Generalized Inference*, Metrologia, Volume 42, Number 2, April 2005, pp. 145-153.

The ISO Guide to the Expression of Uncertainty in Measurement (GUM) recommends the use of a first-order Taylor series expansion for propagating errors and uncertainties. The GUM also endorses the use of 'other analytical or numerical methods' when the conditions for using the Taylor expansion do not apply. In this paper we propose an alternative approach for evaluating measurement uncertainty based on the principle of generalized inference. The proposed approach can be applied to measurement models having any number of input quantities and a vector-valued measurand. We use several examples from the GUM to illustrate the implementation of the proposed approach for the calculation of uncertainties in measurement results.

Wang, Q., Ressler, S., *A Tool Kit to Generate 3D Animated CAESAR Bodies*, 2005 SAE Digital Human Modeling for Design and Engineering Symposium, Iowa City, Iowa, June 14, 2005

The Civilian American and European Surface Anthropometry Resource (CAESAR) database provides a comprehensive source for body measurement in numerous industries such as apparel, aerospace, and automobile. Generating animated CAESAR body sequences from still surface and landmark data will stimulate research and design in these areas. A tool kit has been developed to convert CAESAR bodies to models compliant with the Humanoid Animation specification (H-Anim). It will be helpful to set up a realistic motion capable humanoid library for application environment that can be reused in a wide variety of ergonomic applications. The process consists of preprocessing the mesh, building a skeleton structure, creating segments of the body, assigning weights for vertices, and integrating motion capture data. Publicly available software is adopted for mesh compression and hole filling. C programs were developed to implement the translation from CAESAR body data to H-Anim. The technical issues involved in the process are discussed, and experimental results are shown in the paper.

Wang, Q., Saunders, B., *Web-Based 3D Visualization in a Digital Library of Mathematical Functions*, NISTIR 7159 and Proceedings of the WEB3D 2005 Symposium, University of Wales, Bangor, UK, March 29-April 1, 2005, pp. 151-157.,

The National Institute of Standards and Technology (NIST) is developing a digital library of mathematical functions to replace the widely used National Bureau of Standards Handbook of Mathematical Functions published in 1964 [1]. The NIST Digital Library of Mathematical Functions (DLMF) will provide a wide range of information about high-level functions for scientific, technical and educational users in the mathematical and physical sciences. Clear, concise 3D visualizations that allow users to examine poles, zeros, branch cuts and other key features of complicated functions will be an integral part of the DLMF. Specially designed controls will enable users to move a cutting plane through the function surface, select the surface color mapping, choose the axis style, or transform the surface plot into a density plot. To date, Virtual Reality Modeling Language and Extensible 3D (VRML/X3D) standards have been used to implement these capabilities in more than one hundred 3D visualizations for the DLMF. We discuss the development of these visualizations, focusing on the design and implementation of the VRML code, and show several examples.

Watson, C., Wilson, C., Marshall, K., Indovina, M., Snelick, R., *Studies of One-to-One Fingerprint Matching with Vendor SDK Matchers*, NISTIR 7221, http://fingerprint.nist.gov/SDK/, April 2005,

NIST has conducted testing of one-to-one SDK (Software Development Kit) based COTS (Commercial Off-The-Shelf) fingerprint matching systems to evaluate the accuracy of one-to-one matching used in the US-VISIT program. Fingerprint matching systems from eleven vendors not used in US-VISIT were also evaluated to insure that the accuracy of the matcher tested was comparable to the most accurate available COTS products. The SDK based matching application was tested on 20 different single finger data sets of varying difficulty. The average true accept rate (TAR) at a false accept rate (FAR) of 0.01% was better than 98% for the two most accurate systems while the worst TAR at a FAR of 0.01% was greater than 94%. The data sets used and the ranking of the systems are discussed in detail in the report. A copy of this report and appendices are available at http://fingerprint.nist.gov/SDK.

Watson, C., Wilson, C.L., *Effect of Image Size and Compression on One-to-One Fingerprint Matching*, NISTIR 7201, http://www.itl.nist.gov/iaui/894.03/pact/pact.html, February 2005

NIST has conducted testing of one-to-one fingerprint matching systems to evaluate the effect of image size and compression on the accuracy of the one-to-one matching process. Images from three live-scan fingerprint scanners collected by the Departments of State and Homeland Security were used as test samples. Image sizes from 368 pixels by 368 pixels down to 180 pixels by 180 pixels were tested and compression ratios from no compression up to 30 to 1 were tested. Three commercial fingerprint-matching systems were used in the test. The results of the study show that image cropping quickly degrade matcher performance. Compression degrades matcher performance more slowly and may, for compression ratios of 15 to 1, increase performance. Image sizes below 320 by 320 should not be used. Image compression in the range up 20 to 1 produces minimal effects on fingerprint matching accuracy.

Watson, C.I., Wilson, C.L., Indovina, M., Cochran, B.J., *Two Finger Matching with Vendor SDK Matchers*, NISTIR 7249, http://www.itl.nist.gov/iaui/894.03/pact/pact.html, July 2005

This report is an extension of the NIST "Studies of one-to-one Fingerprint Matching with Vendor SDK Matchers" which evaluated the accuracy of SDK (Software Development Kit) based on COTS (Commercial Off-The-Shelf) fingerprint matching systems for one-to-one verification applications. Fingerprint matching systems from twelve vendors were evaluated. The two finger matching evaluation is an extension of that testing used to evaluate the accuracy that can be achieved by combining the index finger scores to achieve a match. These results are based on the SDK matchers provided for the original single finger SDK testing. More details will be available from the Minutiae Exchange Test 2004 (MINEX04) http://fingerprint.nist.gov/MINEX04. The more accurate matchers in the two finger SDK scoring were able to achieve true accept rates (TAR) in the range of .985 - .998 at a false accept rate (FAR) of 0.0001. A copy of this report and appendices is available at http://fingerprint.nist.gov/SDK.

White, D., Tebbutt, J., *A Perl-Based Framework For Distributed Processing*, Open Source Developers' Conference 2004, Melbourne, Australia, December 1, 2004

The National Software Reference Library (NSRL) of the U.S. National Institute of Standards and Technology (NIST) collects software from various sources and publishes file profiles computed from this software (such as MD5 and SHA-1 hashes) as a Reference Data Set (RDS) of information. The RDS can be used in the forensic examination of file systems, for example, to speed the process of identifying unknown or suspicious files. This paper describes the cross-platform, public domain, Linux/Apache/MySQL/Perl (LAMP) framework with which we produce the RDS from acquired software. The framework is easily deployed (it has been packaged on a Knoppix-based live CD) and allows for the distributed processing of large numbers of files in a loose, heterogeneous computing cluster. We go on to suggest that the framework is sufficiently general in its implementation to be suitable for application to classes of problems quite beyond our original scope.

Wilson, C., Grother, P., Chandramouli, R., *Biometric Data Specification for Personal Identity Verification*, NIST SP 800-76, http://csrc.nist.gov/publications/nistpubs/index.html

The Homeland Security Presidential Directive HSPD-12 called for new standards to be adopted governing the interoperable use of identity credentials to allow physical and logical access to Federal government locations and systems. The Personal Identity Verification (PIV) for Federal Employees and Contractors, Federal Information Processing Standard (FIPS 201) was developed to establish standards for identity credentials. This document, Special Publication 800-76 (SP 800-76), is a companion document to FIPS 201. It specifies technical acquisition and formatting requirements for the biometric credentials of the PIV system, including the PIV Card1 itself. It enumerates required procedures and formats for fingerprints and facial images by restricting values and practices included generically in published biometric standards. The primary design objective behind these particular specifications is universal interoperability. For the preparation of biometric data suitable for the Federal Bureau of Investigation (FBI) background check, SP 800-76 references FBI documentation, including the ANSI/NIST Fingerprint Standard and the Electronic Fingerprint Transaction Sets.

Wu, J.C., Wilson, C.L., *Nonparametric Analysis of Fingerprint Data*, NISTIR 7226, http://www.itl.nist.gov/iaui/894.03/pact/pact.html, May 2005, and Pattern Recognition, to be published

This paper demonstrates that, for large-scale tests, the match and non-match similarity scores have no specific underlying distribution function. The forms of these distribution functions require a nonparametric approach for the analysis of the fingerprint similarity scores. In this paper, we present an analysis of the discrete distribution functions of the match and non-match similarity scores of the fingerprint data that clarifies the widely varying form of these distribution functions. This analysis demonstrates that a precise Receiver Operating Characteristic (ROC) curve based on the True Accept Rate (TAR) of the match similarity scores and the False Accept Rate (FAR) of the non-match similarity scores can be constructed without any assumption regarding operating thresholds or the form of the distribution functions. The area under such a ROC curve, assuming normality, is equivalent to the Mann-Whitney statistic directly formed from the match and non-match similarity scores. In addition, the Z statistic computed using the areas under ROC curves along with their variances is applied to test the significance of the difference between two ROC curves. Four examples than from NIST's extensive testing of commercial fingerprint systems are provided. The nonparametric approach presented in this article can also be employed in the analysis of other biometric data.

Yanik, L., Torre, E.D., Donahue, M.J., Cardelli, E., Micromagnetic Eddy Currents in Conducting Cylinders, Journal of Applied Physics, accepted for publication

The inclusion of eddy currents into micromagnetic programs is important for the proper analysis of dynamic effects in conducting magnetic media. This paper introduces a limited numerical implementation for eddy current calculations and discusses some interesting analytic cases in the simplified geometry. It is designed to provide some benchmarks for more complex program.

Yanik, L., Torre, E.D., Donahue, M.J., *Micromagnetic Calculations of Eddy Currents with Time-Varying Fields*, Physica B, to be published

This paper extends a recently presented program for solving the eddy current problem in a cylindrical geometry, by investigating the effect of time-varying fields. When the applied field is turned off, wall motion slows by several orders of magnitude, but since the wall energy can be reduced by reducing the length of the wall, it continues to move, albeit much more slowly. Reversing the applied field has the effect of nucleating the opposite kind of wall which propagates inward and eventually annihilates the previous wall.

Zhang, N. F., Strawderman, W. E., Liu, H. K., Sedransk, N., *Statistical Analysis for Multiple Artifact Problem in Key Comparisons With Linear Trends*, Metrologia, to be published

A statistical analysis for key comparisons with linear trends and multiple artifacts is proposed. This is an extension of a previous paper for a single artifact. The approach has the advantage that it is consistent with the no-trend case. The uncertainties for the key comparison reference value and the degrees of equivalence are also provided. As an example, the approach is applied to key comparison CCEM-K2.

Zhang, N.F., *Statistical Analysis on Uncertainty for Autocorrelated Measurements*, Metrologia, to be published

When repeated measurements are autocorrelated, it is inappropriate to use the traditional approach to calculate the uncertainty of the average of the measurements, which assumes that the measurements are statistically independent. In this paper, we propose a practical approach to calculate the corresponding uncertainty and the confidence interval when the data are from a stationary process. For illustration, the approach is applied to linewidth measurements made by a scanning electron microscope.

Zhang, N.F., *Statistical Process Control in Biochemical and Hematological Quality Control Data*, Proceedings of the American Statistical Association, to be published

Daily quality control (QC) measurements of common biochemical and hematological quantities were recorded during several months while methods and analyzers showed no signs of malfunctioning. Usually it is assumed that QC data may be described as i.i.d. In this case an X chart and/or an EWMA chart are the proper control charts to use. When autocorrelation is presented, the traditional control charts may be inefficient. An alternative control chart, the EWMAST chart proposed in Zhang (1998) has been developed for stationary process data. The EWMA and the EWMAST chart were applied to each of the 11 QC data series. In 6 of the 11 series, significant process autocorrelations were demonstrated. The results show that the conventional EWMA chart may give false alarms in the presence of autocorrelation while the EWMAST chart gave few false alarms.

Zhang, N.F., Winkel, P., *The Effect of Recalibration and Reagent Lot Changes on the Performance of QC Control Charts*, Clinical Chemistry, to be published

Daily QC measurements of biochemical quantities were recorded during four to five months while methods and analyser showed no signs of malfunctioning. The time series of QC values were divided into subseries according to reagents or electrolyte diluent lot and (within diluent subseries) disposable electrode used. ANOVA was used to examine if the mean level changed significantly between subseries. All time series, as well as reagents and diluent subseries were examined for autocorrelation. The X-chart and the EWMAST (in autocorrelated series) or EWMA chart were applied to each time series and each reagents and diluent subseries and the number of values falling outside the 3 SD control limits were noted. Results: The mean levels changed significantly due to diluent lot changes, replacement of disposable electrodes and recalibrations following reagents lot changes. These changes caused spurious autocorrelation as evidenced by the ACF plot. In 42% of all reagents subseries a significant autocorrelation could also be demonstrated; however, 5.64% and 29.1% of all time series values fell outside the control limits of the X-charts and the EWMA or EWMAST charts respectively. These percentages were reduced to 0.44 and 0.7 when separate control charts were calculated following recalibrations and changes of diluent lot. Conclusions: The mean level may change due to recalibrations and change of electrode diluent lot that causes an excessive number of false alarms unless new control charts are calculated subsequent to these events.

Ziring, N., Wack, J., *Specification for the Extensible Configuration Checklists Definition Format (XCCDF)*, NISTIR 7188, http://csrc.nist.gov/checklists/docs/xccdf-spec-1.0.pdf, January 2005

This document specifies the data model and XML representation for the Extensible Configuration Checklist Description Format. An XCCDF document is a structured collection of security configuration rules for some set of target systems. The XCCDF specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. The specification also defines a data model and format for storing results of benchmark compliance testing. The intent of XCCDF is to provide a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance, and thereby foster more widespread application of good security practices.