Information Technology Laboratory

Technical Accomplishments

2004

Building Trust and Confidence in IT through Standards, Measurements, and Technology

NISTIR 7169

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

C O N T E N T S

NISTIR 7169
February 2005

U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary

Technology Administration
Phillip J. Bond
Under Secretary of Commerce for Technology

National Institute of Standards and Technology
Hratch G. Semerjian, Jr., Acting Director

About ITL

For more information about ITL, contact:

Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900

Telephone: (301) 975-2900
Facsimile: (301) 840-1357
E-mail: itlab@nist.gov
Website: *http://www.itl.nist.gov*

DIRECTOR'S FOREWORD

In today's complex technology-driven world, the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology has the broad mission of supporting U.S. industry, government, and academia with measurements and standards that enable new computational methods for scientific inquiry, assure IT innovations for maintaining global leadership, and re-engineer complex societal systems and processes through insertion of advanced information technology. Through its efforts, ITL seeks to enhance productivity and public safety, facilitate trade, and improve the quality of life. ITL achieves these goals in areas of national priority by drawing on its core capabilities in cyber security, software quality assurance, advanced networking, information access, mathematical and computational sciences, and statistical engineering.

Dr. Shashi Phoha, Director, Information Technology Laboratory

Information technology is the acknowledged engine for national and regional economic growth. The push for its adoption in all sectors is overwhelming. The insertion of advanced technologies at national or global scales, like biometric identification for entry into the United States or electronic patient records to effectively decrease medical errors, often disrupts established social processes and interacts with other complex societal systems in unpredictable ways. ITL researchers have developed detailed protocols and operational standards that mitigate anticipated discrepancies in their operation, and established assessment criteria and test data sets for validation of industrial products. Specific challenges are addressed through several legislative mandates, ITL has been charged to lead the nation in utilizing existing and emerging IT to meet national priorities that reflect the country's broad based social, economic, and political values and goals. In 2004, ITL continued to fulfill its extended charge under the Federal Information Security Management Act to develop cybersecurity standards, guidelines, and associated methods and techniques. Charged under other legislation, such as the USA PATRIOT Act and the Help America Vote Act, ITL is addressing the major challenges faced by the nation in the areas of homeland security and electronic voting.

In the past decade, advances in computing and communications technologies have unleashed the power of the Internet and forever changed the landscape for commerce and government. ITL

has played an important role in facilitating this transformation. In 2004, we continued our efforts by establishing test beds to formulate and evaluate first responder indoor localization techniques for building safety. In collaboration with the ANSI accredited standards organization Health Level 7 (HL7), ITL also led the development of electronic health records and messaging standards that promote a secure and reliable healthcare environment. Last year also saw ITL champion the successful establishment of national and international biometric consensus standards bodies. ITL will continue to contribute in numerous other ways to enable the transition of information technologies to meet today's challenges.

Information is not a physical entity but, similar to the physical world, appropriate metrology is needed to guide its broad application. Within NIST's traditional role as the overseer of the National Measurement System, ITL is addressing the hard problems in IT Measurement Research. ITL formulates metrics, tests, and tools for a wide range of subjects such as information complexity and comprehension (to cope with information overload), high confidence software (to cope with information reliability), space-time coordinated mobile and wireless computing (to cope with information availability), as well as, issues of information quality, integrity, and usability. These hard problems are some of the Grand Challenges identified in the FY 2004 Interagency Coordination Report by the National Information Technology Research and Development (NITRD) Program that seeks to accelerate progress towards national goals. In 2004, ITL made strides toward these goals by drafting public key management schemes and guidelines for authenticated encryption modes that will improve the security of systems within and outside the Government. ITL also reached out to federal agencies and industry through development of security guidelines in areas where they were most needed, such as, personal digital assistant (PDA) forensics, Windows XP, Voice-over-Internet-Protocol (VOIP), smart card technology and many others. ITL worked with the World Wide Web Consortium (W3C) to release test suites for XML that have become the de facto metric for assessing quality of the XML products that enable electronic commerce. These efforts highlight the broad influence that our software testing and security programs are having on assessment and accreditation of new products and technologies and on making information secure throughout the Government; helping to ensure continuity and safe operation of the national information infrastructure that underlies economic competitiveness and homeland security.

ITL is also engaged in preparing the nation for the next phase of the Information Revolution. Drawing on the two great revolutions of the twentieth century, Quantum Physics and Computer Science, NIST has formulated its Quantum Information Program to transform both computing and secure communications. In collaboration with NIST's Physics and Electronics and Electrical Engineering Laboratories, ITL is exploiting quantum mechanics, the strange behavior of matter on the atomic scale, for making cryptographic codes that are unbreakable even by the supercomputers of tomorrow. This technology can also be exploited to break cryptographic codes in seconds that could not be cracked in a million years by the most powerful binary computers. The need for the U.S. to stay at the forefront of this technology is critical to future homeland security. In 2004, we established quantum computing and communications test beds to demonstrate the exchange of sifted quantum cryptographic keys at the rate of 3.5Mbps—two orders of magnitude faster than the previous record, and, realized the first experiment to reliably "teleport" quantum states between atoms as reported in the June 17, 2004 issue of *Nature*. These and other ITL efforts will shape the next generation of information technology and cybersecurity.

ITL seeks to scale new frontiers in Information Measurement Science to enable international social, economic, and political advancement. Issues of trade, public health and safety, energy, pollution and transportation span across national boundaries and depend heavily on the critical IT infrastructure. Lack of objective measurements often hinders the universal applicability of U.S. technology and acts as a trade barrier, limiting the reach of U.S. commerce. In 2004, ITL collaborated and partnered with industry, academia, and other NIST laboratories to advance science and engineering, setting standards and requirements for unique scientific instrumentation and experiments, data, and communications. ITL also enabled breakthroughs in research through immersive visualization in areas such as tissue engineering and nanostructures. ITL continues to lead the way in enabling innovations in interdisciplinary sciences and ensuring their international applicability.

I am proud to highlight many outstanding achievements of ITL's talented staff members and cross-cutting interdisciplinary research programs. ITL researchers have taken leadership roles and served with distinction in both national and international standards development committees promoting the interests of many essential U.S. industries.

Thank you for your interest in the Information Technology Laboratory. Please take a few minutes to review this document and visit our website at www.itl.nist.gov to learn more about how ITL is enabling the future by innovating the IT measurement and standards infrastructure.

Shashi Phoha

Dr. Shashi Phoha, Director
Information Technology Laboratory
E-mail: itlab@nist.gov

ITL AT A GLANCE

Kamie Roberts, Acting ITL Deputy Director

OUR CORE PURPOSE

Enabling a better future through information technology (IT).

OUR MISSION

To support U.S. industry, government, and academia by enabling new computational methods of scientific inquiry, assuring IT innovations for maintaining global leadership, and re-engineering complex societal systems and processes through insertion of advanced information technology.

OUR VISION

To be the global leader in developing the relevant measurement science for advancing information technology and bringing its benefits to society.

OUR MANAGEMENT TEAM

Shashi Phoha, *ITL Director*

Kamie Roberts, *Acting ITL Deputy Director, Associate Director for Federal and Industrial Relations*

Bradley Alpert and Jack Wang, *Acting Assistant Directors for Boulder*

Kendra Cole, *Senior Management Advisor*

Ronald Boisvert, *Chief of Mathematical and Computational Sciences Division*

David Su, *Chief of Advanced Network Technologies Division*

Edward Roback, *Chief of Computer Security Division*

Martin Herman, *Chief of Information Access Division*

Mark Skall, *Chief of Software Diagnostics and Conformance Testing Division*

Nell Sedransk, *Chief of Statistical Engineering Division*

OUR RESOURCES

- highly qualified professional and support staff of 313 (includes part-time, students, and faculty appointments), and 147 guest researchers (as of September 30, 2004)
- total authorization for fiscal year 2004 budget of $71.9M, all sources (as of September 30, 2004)
- research and operations facilities in Gaithersburg, Maryland, and Boulder, Colorado
- opportunities for cooperative research and interaction with industry and academia

OUR PRODUCTS AND SERVICES

- reference data sets and evaluation software
- standards
- proof-of-concept implementations
- advanced software quality assessment tools
- automated software testing techniques
- tests, test tools and methods
- statistical model-based testing
- specialized databases
- electronic information on the web
- mathematical and statistical consulting services

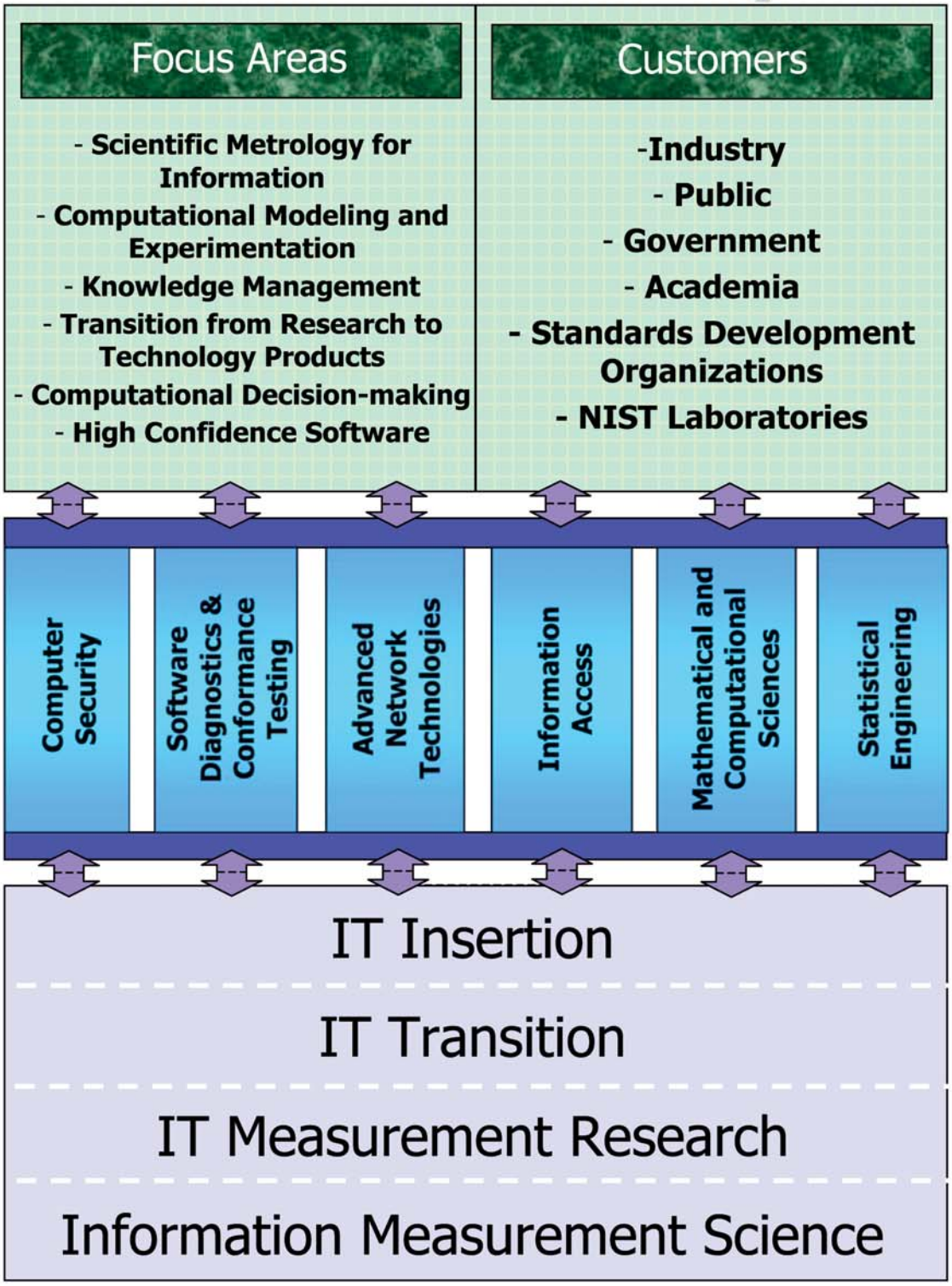
OUR CUSTOMERS

- U.S. industry
- federal agencies
- academia
- NIST staff and collaborators
- research laboratories
- IT users and providers
- industry standards organizations

OUR RESEARCH PROGRAM

Our research program is rooted in the development of relevant measurement science for guiding the advancement and insertion of information technology in societal processes. The following chart presents the ITL Research Blueprint, the framework by which we describe our research program. The spectrum of ITL contributions connects IT Insertion, IT Transition, IT Measurement Research, and Information Measurement Science to our technical focus areas and our customers.

ITL Research Blueprint

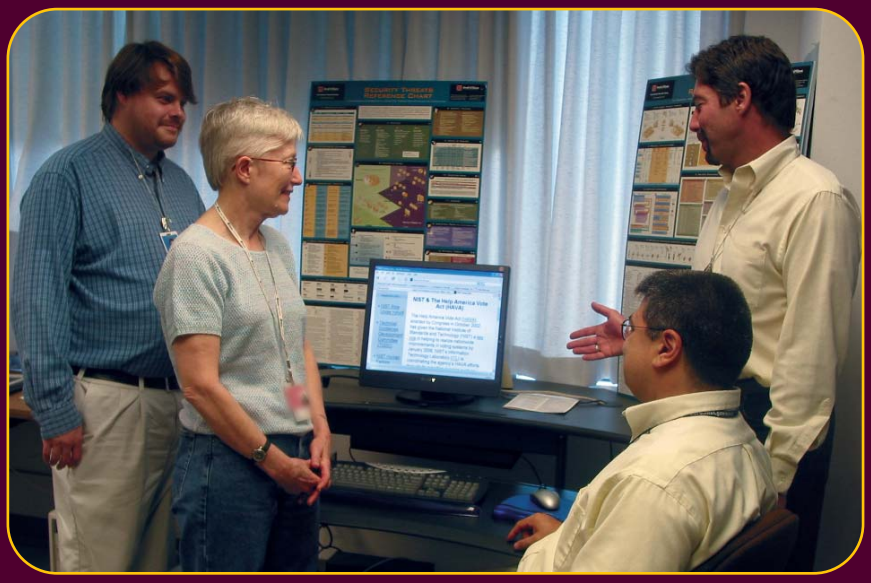


ACCOMPLISHMENTS
OF OUR RESEARCH PROGRAM

ITL computer scientist Ross Micheals demonstrates a NIST-developed system for studying the performance of facial recognition software programs. The system takes a person's photo with nine cameras from different angles. The photos are then analyzed by commercial facial recognition systems to see whether using many high-resolution digital photographs can improve performance. NIST will use results from the research in support of its Congressional mandate under the USA PATRIOT Act to certify the use of biometrics such as digitized photos and fingerprints in passports and visas.

FOUNDATION RESEARCH AREAS

SECURITY



John Kelsey (left), Annabelle Lee, Nelson Hastings (seated), and John Wack examine e-voting security issues in support of the Technical Guidelines Development Committee.

SECURITY TECHNOLOGY

Federal agencies and private sector organizations are selecting cryptographic security components and functionality for protecting their data, communications, and operations, from ITL's comprehensive cryptographic toolkit, which includes a wide variety of cryptographic algorithms and techniques for protecting the integrity, confidentiality, and authenticity of information resources. Program areas include cryptographic standards, key management, public key infrastructure (PKI), identity management, e-authentication, and agency e-government support. The website is *http://csrc.nist.gov/CryptoToolkit/index.html*.

Our accomplishments in FY 2004 included many significant draft documents, standards, and validation tests. We wrote a draft key management schemes document and guidelines on a recommendation for authenticated encryption modes for public review. We revised the Digital Signature Standard (DSS) in preparation for public review and comment and developed validation tests for authentication, the Digital Signature Algorithm (DSA), the Secure Hash Algorithm (SHA), the Keyed-Hash Message Authentication Code (HMAC), and American National Standards Institute (ANSI) X9.62, *Public Key Cryptography for the Financial Services Industry*. We conducted a successful workshop on Random Number Generation (RNG) and developed a draft RNG Standard (ANSI X9.82.)

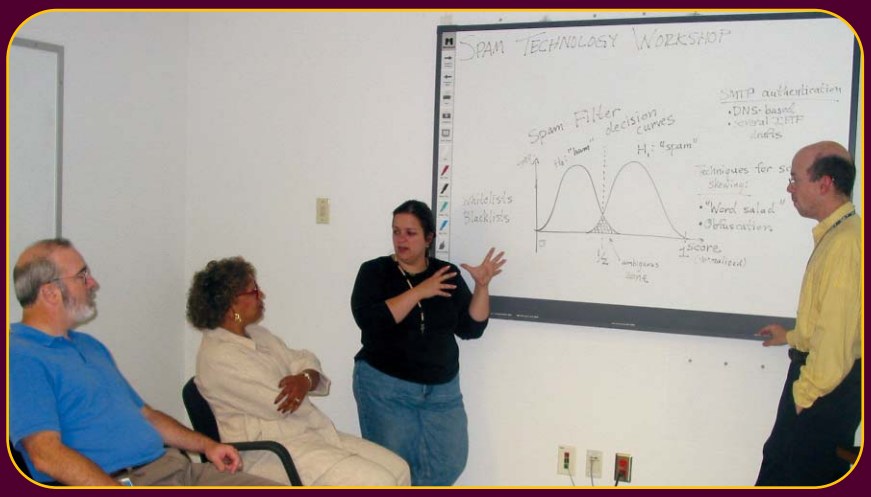
In the area of e-authentication, we published our guideline on electronic authentication and initiated development on a NIST recommendation on password usage. We developed credential service providers accreditation criteria and supported the integration of the Federal Bridge Certification Authority with governmentwide e-authentication efforts. We sponsored a workshop to discuss requirements, terminology, components, and metrics of knowledge-based authentication (KBA) and developed a white paper on metrics for KBA. We also provided leadership for international biometric data interchange and interoperability standards, including the common Biometric Exchange Formats Framework (CBEFF) specification and guidelines (see Biometrics).

Our work in cryptography is making an impact within and outside the federal government. Strong PKI and cryptography improve the security of systems and the information they process. IT users also enjoy the enhanced availability in the marketplace of secure applications through cryptography, PKI, and e-authentication. See *http://csrc.nist.gov/pki*.

SYSTEMS AND NETWORK SECURITY

We continued our robust technical program to protect information systems and the networks that connect them. Our technical guidelines and standards, publications, *ITL Bulletins*, checklists, online resources, and specifications address a wide range of critical systems and network security areas. Federal agencies rely on the NIST technical guidelines, which are frequently cited and reused by industry on a voluntary basis.

In FY 2004, we published technical guidance on personal digital assistant forensics, developing security checklists, securing Windows XP, mapping types of information and information systems to security categories, computer security incident handling, network security testing, voice over Internet protocol (VOIP) security, card technology, and IT security products and services. Eleven *ITL Bulletins* were published on security matters spanning technical, managerial, and operational security issues; these bulletins are widely read inside and outside of the federal government.



Mark Wilson (seated), Joan Hash, Tanya Brewer-Joneas, and David Griffith discuss ITL's SPAM Technology Workshop held on February 17, 2004.

The Multi-mode Authentication Framework effort implemented several authentication mechanisms including Picture Password, a Smart Multi-Media Card mechanism, a Bluetooth Smart Card mechanism, and a Wireless Proximity Beacon mechanism. We developed extensions to an open source windowing software for Linux handhelds (i.e., OPIE) that support multi-mode authentication and a common interface for authentication modules. We provided forensics investigators with draft guidelines, documentation, and proper techniques for investigating digital handheld devices. We developed a standard access control model and mechanism capable of being configured in support of any attribute-based access control policy (to include policy combinations) and the ITL-developed RBAC Standard, ANSI INCITS 359-2004, was adopted as a national standard.

Other accomplishments included the development of a proof-of-concept implementation of a secure routing protocol based on Ad-hoc On-Demand Distance Vector (AODV) over IPv6, further reinforced by a routing protocol-independent Intrusion Detection and Response system for ad-hoc networks. The online ICAT vulnerability database was enhanced and now contains about 7,000 entries. ICAT enables system administrators to identify flawed systems and to find the patches. We provided the technical specifications for a new suite of international smart card standards. On the national level, ITL led the establishment of a new ANSI task group to develop a national standard for smart card interoperability. Both work efforts are based on NIST InterAgency Report 6887, *Government Smart Card Interoperability Specification (GSC-IS), v2.1*. Websites are *http://csrc.nist.gov/publications/*, *http://icat.nist.gov/icat.cfm*, *http://smartcard.nist.gov*, and *http://csrc.nist.gov/rbac/*.

MANAGEMENT AND ASSISTANCE

An important component of our computer security program is our outreach, expert assistance, policy, and guidelines for federal agencies, industry, and small and medium-size businesses. We direct our new guidelines development efforts where they are most needed, in areas identified by such advisory groups as the Information Security and Privacy Advisory Board, which we support. We also host the Federal Computer Security Program Manager's Forum quarterly meetings to provide insight to and receive feedback from the federal community.

In FY 2004, we developed several significant new guidance documents, including security considerations in the information system development life cycle, a resource guideline for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,

and Integrating Security into the Capital Planning and Investment Control Process. Based on agency feedback, we reinvented our Computer Security Expert Assist Team (CSEAT) as the Program Review for Information Security Management Assistance (PRISMA, http://prisma.nist.gov) to better serve federal agencies that request security program reviews. We also improved and maintained our Computer Security Resource Center (CSRC), one of the most visited websites at NIST: *http://csrc.nist.gov*.

Our support of small and medium-sized businesses continued. We updated the small business corner of our CSRC website. We grew community college and Small Business Development Corporation participation to the national level, making NIST a viable information security resource for existing, localized, small business support infrastructure. We also launched a NIST Small Business Administration InfraGard Small Business Resource Group. The website is *http://sbc.nist.gov/*.

SECURITY TESTING AND METRICS

Our security testing and metrics program provides our customers with a proven set of IT security services based on sound testing methodologies and test metrics. Program components include the Cryptographic Module Validation Program (CMVP), Cryptographic Module Testing Laboratory accreditation, the Cryptographic Algorithm Validation Program (CAVP), the National Information Assurance Partnership (NIAP), and certification and accreditation of information systems.

The CMVP provides federal agencies in the United States and Canada with confidence that a validated cryptographic product correctly implements government cryptographic standards (http://csrc.nist.gov/cmvp). In FY 2004, the CMVP validated over 200 individual cryptographic modules and assisted in the technical accreditation of three new Cryptographic Module Testing (CMT) Laboratories. Two CMT laboratories were reaccredited, as were three common criteria laboratories. We continued our work in the International Organization for Standardization for the international adoption of Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*. We supported a national level review of NIAP called for by the White House in the *National Strategy to Secure Cyberspace*. In response to a mandate under the Federal Information Security Management Act of 2002, we produced FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and a guideline for the *Security Certification and Accreditation of Federal Information Systems*. We also published a draft of *Minimum Recommended Security Controls for Information Systems* guideline and initiated the draft of a companion validation document.

ITL's information security program is making a significant impact, especially in the increased security of IT systems through the availability of tested products. Our program also creates business opportunities for security product vendors, testing laboratories, security consultants, and small businesses. ■

(From left) Marianne Swanson, Ray Snouffer, Peggy Himes, Curt Barker, Gary Stoneburner, Ron Ross, Stu Katzke, Joan Hash, Arnold Johnson, and Annabelle Lee (not pictured) review the many draft security requirements being developed by ITL in response to Congressional assignments in the Federal Information Security Management Act (FISMA) of 2002.

SOFTWARE

Trusted, high-quality software is often taken for granted and not noticed until it fails. Software with bugs causes software to be unreliable and often means hidden security vulnerabilities. Software quality relies on precise, testable software standards, followed by the development of conformance test suites and tools to help vendors build high-quality, interoperable implementations that meet the needs of the users.

From left) Sydney Henrard, Rob Snelick, Len Gebase, and Clare Witte help improve interoperability of healthcare systems by developing a conformance testing framework for exchanging health information.

ELECTRONIC COMMERCE

The impact of software errors is enormous because virtually every business now depends on software for the development, production, distribution and after-sales support of products and services. To facilitate electronic commerce, ITL is developing software testing tools and methods that improve quality, conformance to standards, and correctness. Projects include XML Core, XML Schema, XML Query, and Linux. We lead the conformance testing efforts for all of these projects, developing and maintaining the test frameworks and test suites. To improve the development process, we are building an automated method for generating tests based on XML technologies. In FY 2004, we completed and released new tests for XML, Namespaces, XInclude, XML Schema, and XML Query. With the World Wide Web Consortium (W3C), we jointly issued public releases of these test suites. Our test suites have become the metric by which XML products are measured and have been incorporated into several commercial products.

We continued our W3C conformance advisory role, by co-chairing the W3C Quality Assurance (QA) Interest Group and participating in the QA Working Group (WG). We served as editors and major contributors to the QA Guidelines; the W3C WGs used the QA Guidelines to improve their charters, operational processes, and specifications. Additionally, we developed tools to facilitate the creation of a conformance clause within a specification, a W3C Charter, and a QA process document. We applied the guidance we developed on writing better specifications to other standards areas, such as healthcare. Our expertise contributes to higher-quality specifications and test suites.

A related project is the development of a consistent test framework for electronic business XML (ebXML). Working with the Organization for the Advancement of Structured Information Standards (OASIS), we developed an ebXML Test Framework Specification 2.0 and conformance tests for messaging and registry services. To support this framework, we developed a prototype implementation.

Another area of interest is our smart card testing, including basic services interface (BSI) testing and card edge testing for the Government Smart Card (GSC) program. We developed four test suites and are transitioning them to the Joint Interoperability Test Command.

The impact of our conformance testing program is significant. Many software developers use our test suites, resulting in bug fixes to XML implementations and specifications. The test methodologies that we develop influence others, including Open Source Linux, OASIS, SourceForge, Apache, the Korean B2B Interoperability Testbed (KorBIT), the European Telecommunications Standards Institute (ETSI), and the Government Smart Card-Interoperability Specification (GSC-IS). Our XML Tester Tool has been adopted by industry. ITL conformance tests continue to influence all XML software solutions, which are used by millions of consumers. The websites are *http://www.nist.gov/xml*, *http://ebxml-testing.nist.gov*, and *http://smartcard.nist.gov*.

HEALTH INFORMATION TECHNOLOGY

In partnership with the healthcare industry, government agencies, and academia, ITL seeks to improve the quality of healthcare, reduce costs, and provide essential services through the use of information technology. In particular, we have focused our efforts on messaging standards and technologies that move clinical information from system to system, electronic health record standards, and standards awareness. Working closely with the ANSI-accredited Health Level 7 (HL7) Standard Development Organization, we focused on HL7 conformance, HL7 registry, and electronic health record systems (EHR-S). In FY 2004, we continued to develop HL7 conformance definitions through our role as Conformance Special Interest Group co-chair and continued to support the HL7 registry, which has become an integral resource in HL7. We began an effort to develop conformance tests for HL7 v2 profiles and are developing the initial conformance criteria for the EHR-S. Additionally, we are developing conformance tests and tools for the Institute of Electrical and Electronics Engineers (IEEE) 1073 Medical Device Communications standard. See *http://www.nist.gov/ehealth*.

Achieving the vision of integrated healthcare environments requires the integration of many clinical, administrative and IT standards. In FY 2004, we collaborated with HL7 and the Healthcare Information and Management Systems Society's (HIMSS) Integrating the Healthcare Enterprise (IHE) project and developed a registry implementation that provided critical infrastructure services at the HIMSS 2004 Demonstration and Conference. We continue to work with IHE, co-authoring the Cross-Enterprise Clinical Documents Sharing profile, which enables the sharing of clinical documents across health enterprises. To support this and other IHE profiles, we developed a prototype implementation, which will serve as the cornerstone of next year's HIMSS Demonstration.

We actively participate in the ANSI Health Informatics Standards Board, eGOV Consolidated Health Informatics, and the American Telemedicine Association (ATA). With the ATA, we conducted a series of workshops to identify standards needed to provide ocular care through telecommunications technology, resulting in an ATA Technical Standard that identifies the appropriate standards, clinical protocols, and administrative guidelines as well as describing the methodology for developing a portfolio of standards. To advance awareness of healthcare standards, we developed a prototype web-based Healthcare Standards Landscape where information on healthcare standards, and organizations developing, promoting, or using these standards can be searched. In FY 2004, we refined the prototype, added new information, and made it publicly available for trial use. The work is being supported by the Agency for Health Research and Quality. The website is *http://hcsl.sdct.nist.gov/*.

COMPUTER FORENSICS

Sound computer forensics practices are key to finding and delivering court-admissible evidence when computers are used in the commission of a crime. Our computer forensics program consists of the National Software Reference Library (NSRL) and the Computer Forensics Tool Testing (CFTT) project. Both projects are coordinated by the NIST Office of Law Enforcement Standards and supported by the National Institute of Justice, the Federal Bureau of Investigation, the Department of Homeland Security, and the Department of Defense. Additional research is done in partnership with the National Archives and Records Administration.

The NSRL is a reference data set of file signatures (hashes) of commercial, off-the-shelf (COTS) files, which can be used during examination of digital evidence to identify pertinent files and eliminate others. The NSRL data set can

eliminate 40-95 percent of COTS files from examination and save hundreds of staff-hours. In FY 2004, we continued to update and populate the NSRL, adding 25 million file signatures for a total of 43 million. Our CFTT project provides a measure of assurance that the tools used in computer forensics investigations produce accurate results. We developed a specification, test methodology, and test software for hard disk write blocking. We delivered test reports to the National Institute of Justice, including four versions of the Royal Canadian Mounted Police tool and two versions from PD Block. We also completed research to support specification and test software for deleted file recovery, string searching, and an expanded disk imaging specification. Our NSRL and CFTT projects have been used in terrorist investigations, including the Moussaoui case and thousands of law enforcement cases. Both projects have received international recognition. The websites are *http://www.nsrl.nist.gov/* and *http://www.cftt.nist.gov/*.

Alden Dima (left) validates the National Software Reference Library Reference Data Set 2.5 and hands it off to Doug White.

GRID COMPUTING SYSTEMS

By connecting hundreds or even thousands of computers together to work on a single project, computer scientists are more frequently using a technique called grid computing to do previously intractable computations. Grid computing systems enable dynamic composition of distributed, heterogeneous resources to perform highly compute-intensive tasks, such as those found in genomics, engineering design, and financial services. Initiated in FY 2004, this project examines current grid standards and systems to improve how computer grids react to volatile conditions. By developing computerized models, we will develop a set of metrics to measure and evaluate robustness and reliability and determine how vulnerable grid networks are to failure. Understanding how grid systems function in volatile environments is critical to the commercial success of this technology. The website is *http://www.itl.nist.gov/div897/docs/gridcomputing.html*.

TEST METHOD RESEARCH

To improve the development of specifications, software tests, and software quality, ITL develops tools and techniques to automate the labor-intensive process of software testing. Our Adaptable and Automated Testing Tools project provides methods for automatically generating tests from specifications and their profiles. This involves the development of test environments that produce self-adapting tests suites that are dynamically created and factor in unique characteristics for defined subsets of a given specification. In FY 2004, we initiated two efforts, Test Accelerator and Adaptable Methods for Testing. The Test Accelerator focuses on building a flexible and extensible test development environment that can generate tests from any specification that can be transformed into our XML-based test language. The Adaptable Methods for Testing focuses on the development of a testing tool and framework to generate self-adapting tests for specification profiles and trading partner agreements that are created at the implementations level. This work is being applied to our conformance test development efforts for XML, Linux, Medical Device Communication, and HL7 conformance. See *http://www.nist.gov/xml/* and *http://www.nist.gov/ehealth/*.

Another area of interest is object oriented (OO) component testing. The goal is to improve software quality, reduce testing costs, and develop reliability estimates that software correctly adheres to its specification. Using our component integration test method, we automated the process of representing the OO specification in databases and generated executable tests. We also developed a Java rapid prototype machine to simulate implementation of the OO specification. See *http://www.itl.nist.gov/div897/docs/software_test_statistical.html*. ■

FOUNDATION RESEARCH AREAS

NETWORKS

Members of the Domain Name System (DNS) Security project devise test and measurement techniques, reference data and technical specifications to improve the robustness of this key component of Internet infrastructure. Pictured (from left) Ramaswamy Chandramouli, Kevin Mills, Steve Quirolgico, Scott Rose, and Doug Montgomery.

INTERNET INFRASTRUCTURE PROTECTION

As the Internet becomes an essential part of day-to-day business operations, security, stability, and availability of Internet services are critical issues to the health of our nation's economy. Expediting the development and deployment of standardized Internet infrastructure protection technologies has been one of ITL's major focus areas in networking. We are developing public specifications to secure the Internet naming infrastructure through our Domain Name System Security (DNSSEC) project. Another effort is the development of standards for the protection of both content and resources in the Internet routing infrastructure, in particular, the Border Gateway Protocol (BGP).

ITL leads the Internet Engineering Task Force (IETF) in the development of several technical specifications for DNSSEC, all of which have reached IETF standards Request for Comments (RFC) status. We also work with industry and the Department of Homeland Security to expedite the deployment of these new standards. These include developing test and measurement framework, tools, and reference data sets for emerging DNSSEC implementations, and for evaluation of the performance impact of security services in large-scale deployments. We also evaluated the BGP threat models and mitigation techniques, and developed simulation and analysis tools to characterize the performance and behavior of BGP under attack in large network configurations. The website is *http://www.antd.nist.gov/iipp.shtml*.

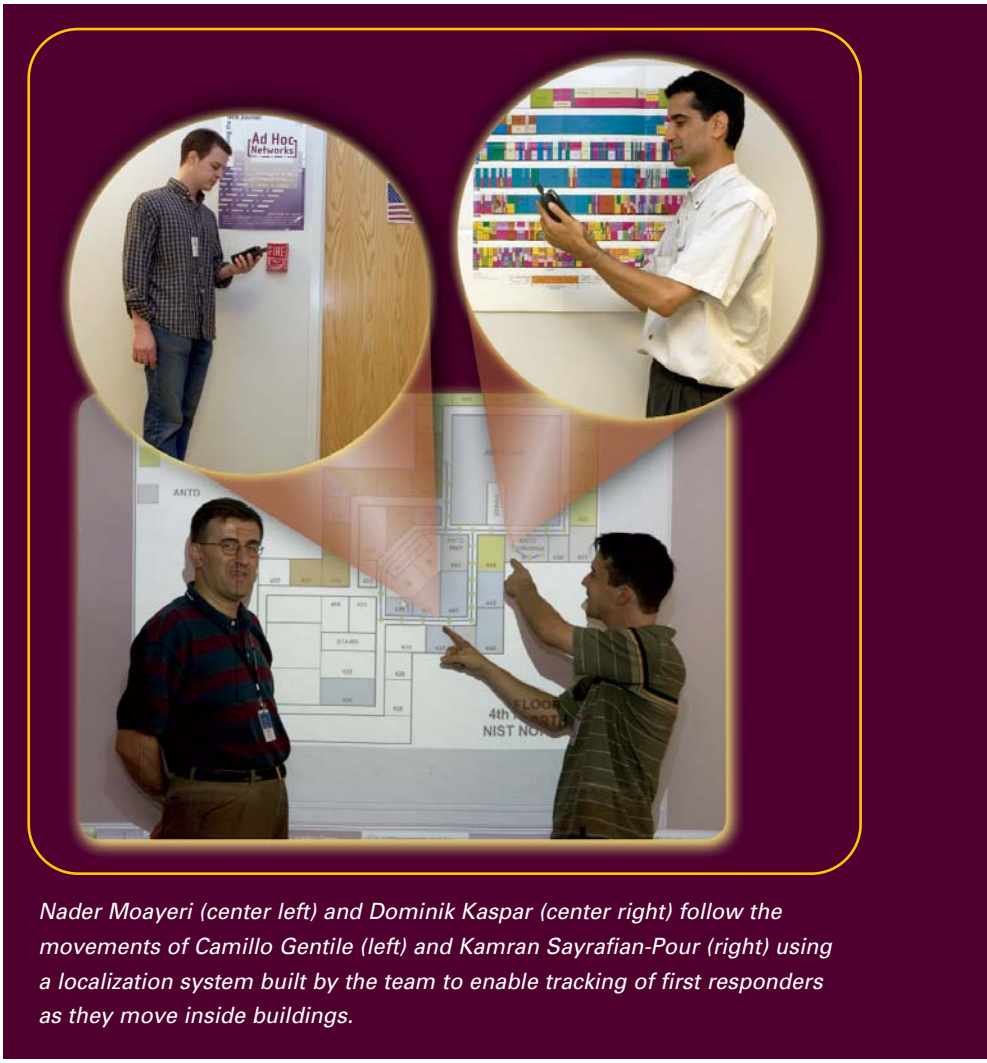
COMMUNICATIONS AND NETWORKING TECHNOLOGIES FOR PUBLIC SAFETY

The reliability and interoperability of communications equipment during emergencies caused by man-made or natural disasters is a critical issue for government agencies in charge of emergency response and public safety. ITL works closely with industry, the first responder and public safety user communities, government agencies, and standards-developing organizations to develop modern, interoperable communications and networking standards in this area. The work includes standards not only for voice communications, but also for a number of other communications and networking capabilities particularly suited to emergency response and public safety operations.

ITL developed a guide on public safety communication technologies that addresses the current, future, and transitional aspects of the use of wireless technology in public

safety communications. The goal is to collect a wide range of useful information about public safety communication technologies in one volume. To expedite development of standards, we participated in the activities of standard organizations, such as Project MESA. We also investigated the transmission of multimedia information in emergency situations using ad hoc network technologies, and developed a real-time simulation tool to evaluate video communications over ad hoc networks under various channel conditions.

In a July 2003 meeting at NIST, about two dozen fire/police chiefs from across the country identified the capability to locate and track movements of first responders inside a building and outdoors within one-meter accuracy as the single most important technology needed for emergency response operations. Therefore, it is crucial to have a neutral, unbiased party to test and evaluate indoor localization techniques and emerging products to sort the facts from the hype. It is also essential to initiate the development of standards for indoor localization.



Nader Moayeri (center left) and Dominik Kaspar (center right) follow the movements of Camillo Gentile (left) and Kamran Sayrafian-Pour (right) using a localization system built by the team to enable tracking of first responders as they move inside buildings.

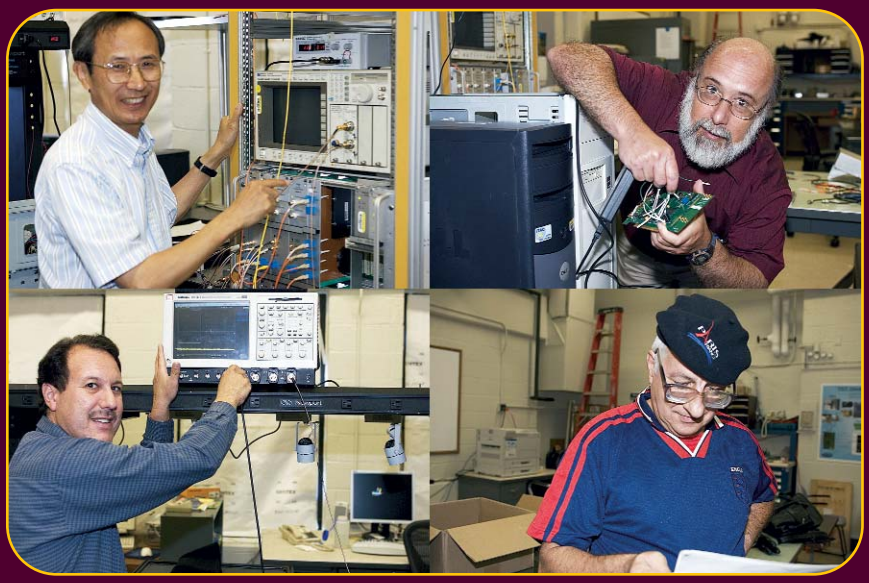
ITL set up a testbed to develop first responder indoor localization solutions, test and evaluate such solutions, and facilitate development of standards for indoor localization. We developed testing methodologies and produced some guidelines, a recommended set of test scenarios, and a common set of performance metrics for performance evaluation of localization techniques. The website is *http://www.antd.nist.gov/comm_net_ps.shtml.*

WIRELESS NETWORK PROTOCOL FOR HEALTHCARE ENVIRONMENTS

Our main objectives in this project are to assist industry in the development of a universal and interoperable wireless interface for medical equipment, expedite the development of standards for wireless technologies, and promote their use in the healthcare environment.

Our current focuses are to understand what existing and emerging wireless technologies can be used in a healthcare environment; to identify related interoperability, security, coexistence, and performance trade-off issues; and to propose protocol changes and devise effective solutions to mitigate these problems.

Working in close collaboration with the Institute of Electrical and Electronics Engineers (IEEE) 1073 Standard Working Group chartered to develop medical device communications and the U.S. Food and Drug Administration, we developed theoretical and simulation models for two candidate Wireless Personal Area Network (WPAN) technologies including the Bluetooth and the IEEE 802.15.4 specifications. We evaluated their performance for several realistic healthcare scenarios and contributed our results to the IEEE 1073 working group. ITL contributions will constitute the basis of standard requirements on the use of wireless communications for medical devices. For more information about this project activity, see *http://www.antd.nist.gov/Health.shtml.*



Xiao Tang (upper left) verifies optical connections, Alan Mink (upper right) connects communication controllers, and Barry Hershman (lower left) configures measurement equipment, while Tassos Nakassis (lower right) reviews code for his error-correction algorithm, as the team prepares to test their quantum key-distribution system, which proved to be the world's fastest.

RESILIENT HIGH-SPEED NETWORKS

ITL's work in this area focuses on developing and evaluating resilient protocols for very high-speed network switching and control architectures. The efforts in making networks more robust consisted of both preventive and reactive measures developed for mitigating physical network failures and cyber attacks and recovering from them.

ITL researchers investigated statistical learning algorithms for detecting anomalies in traffic patterns and effectively demonstrated their use in new and very high-speed network hardware architectures. We also devised a novel theoretical model for evaluating network recovery protocols and determining the optimal mixture and type of resource allocation needed in order to achieve a desired resiliency level.

Working with the IETF, we released several measurement and evaluation tools to the public domain, including a new version of the Generalized Multi-Protocol Label Switching (GMPLS)/Lightwave Agile Switching Simulator (GLASS). For more information on recent results and publications, please visit *http://www.antd.nist.gov/agile_switch.shtml*.

INTERNET TELEPHONY / SIGNALING

Another area of ITL interest is the design and evaluation of technologies to expand the capability and scope of emerging Internet Telephony signaling standards. Projects include the design and development of architectures and standards for programmable Session Initiation Protocol (SIP) signaling stacks and service platforms; the development of security and resource control features to enable emergency signaling and service mobility in SIP-enabled networks; and the evaluation of mechanisms to enable location and context aware call control and applying SIP in wireless ad-hoc networks.

In FY 2003 and continuing into FY 2004, ITL co-designed a new Java Specification (JSR 32) for specifying the interfaces to a SIP Stack. We continued our simulation and analysis of SIP in WANets and published research papers on proposed mechanisms to improve the hand-off performance for mobile users. We designed and prototyped security and resource control mechanisms for programmable active SIP services. We are collaborating with the Java community as experts in the JAIN-SLEE standard (JSR 240) to apply these ideas to emergency telecommunication support for SIP services. We are also collaborating with open source contributors to develop an open source service platform incorporating these ideas. The website is *http://www.antd.nist.gov/it_voip.shtml*.

QUANTUM COMMUNICATIONS TESTBED

ITL worked with other NIST laboratories in the NIST Quantum Communications Testbed program to develop an infrastructure for distribution of quantum encryption keys. We developed a free space link for the quantum channel as well as optical wavelength division channels, and the electronic board and necessary firmware and software for generation, distribution, and use of quantum encryption keys. We achieved a record key exchange rate of 3.5Mbps. (See the Quantum Information section of this report). The website is *http://www.antd.nist.gov/quin.shtml*

FOUNDATION RESEARCH AREAS

Information Access

HUMAN LANGUAGE TECHNOLOGY

By facilitating the creation of relevant measurement methods and standards, ITL is accelerating the development of technologies that allow intuitive, efficient access, manipulation, and exchange of complex information. Projects in human language technology include the Text REtrieval Conference (TREC) series, Advanced Question and Answering for Intelligence (AQUAINT), Translingual Information Detection, Extraction, Summarization (TIDES), automatic content extraction, machine translation, automatic meeting recognition, the Effective, Affordable, Reusable Speech-to-text (EARS) project, and speaker recognition.

(From left) David Pallett, Audrey Tong (standing), Greg Sanders, and Jonathan Fiscus discuss results from Rich Transcription 2004, evaluating the accuracy of automatic speech recognition systems performing speech-to-text transcriptions.

Initiated in 1992, our TREC series is the premier workshop/evaluation series that supports the information retrieval community. In addition to common task-based individual experiments, TREC provides a forum for the exchange of research ideas and a means to accelerate technology transfer. With participation from 103 organizations from 22 countries in FY 2004, TREC 2003 in November 2003 featured six evaluation tracks, including Genomics, Highly Accurate Retrieval from Documents (HARD), Novelty, Question Answering, Robust, and Web. The newly established genomics track brought biomedical and information retrieval communities together for the first time. TREC provides the only test of web search relevance and showed substantial improvement in systems' ability to answer factoid type questions. We prepared for the evaluation tracks for the TREC 2004 in November 2004, performing a web crawl to collect a terabyte data set for the new terabyte track designed to challenge systems to tackle large data problems.

Our related AQUAINT program focuses on advancing the state of the art of question answering to the full range of complex questions asked by humans. In FY 2004, we continued to provide evaluation support for the AQUAINT program and helped define a set of pilot evaluation projects.

In support of the Defense Advanced Research Projects Agency (DARPA) Translingual Information Detection, Extraction, Summarization (TIDES) program, ITL provided evaluation support for the Document Understanding Conference (DUC) 2004. We evaluated generic headline creation and generic summaries of 100 word length and conducted the first cross-language summarization evaluation using multiple Arabic documents as input to a 100-word summary in English. For the TIDES Topic Detection and Tracking (TDT) project, we ran an evaluation for topic detection, presented results in the TDT 2003 Workshop, and prepared for the 2004 evaluation. For the TIDES Machine Translation (MT) project, we ran an evaluation for the MT 2004 workshop evaluating systems that translate Chinese to English and Arabic to English,

including different domain data from previous evaluations. For the DARPA Effective, Affordable, Reusable Speech-to-text (EARS) program, we performed preliminary metadata experiments to determine the target set of metadata to extract, and implemented an evaluation incorporating news program, telephone conversations, and meeting speech.

For the National Security Agency, through our Automatic Content Extraction (ACE) project, we are advancing the state of the art in automatically extracting content from newswire, broadcast news, and newspapers. In FY 2004, we conducted supporting evaluations for the ACE 2004 Workshop. For this we developed evaluation measures and scoring software, and provided analysis of results for Entity Detection and Recognition and Relation Detection and Recognition.

Our Automatic Meeting Recognition (AMR) project was established to explore synergies between audio and visual-based processing to automatically produce rich transcriptions of meetings. The project tackles new challenges in recognizing speech collected from multiple distant microphones and properly transcribing simultaneous highly interactive speech in meeting settings. In 2004, we completed distribution of a 15-hour multimedia pilot meeting corpus and created a 90-minute multi-site test set. We implemented community-wide speech-to-text (STT) and speaker recognition benchmark tests and organized the first Meeting Recognition Workshop.

For our speaker recognition project, we organized a speaker recognition workshop to review evaluation results. We wrote a chapter for a new biometrics book and developed an evaluation plan for 2004. The website is *http://www.itl.nist.gov/iad/programs.html#Human*.

Dorothy Snyder (left), Trudy Cummings, Kathy Gallo, and Pat Flanagan provide outstanding support for IAD's TREC and other technical workshops and evaluation conferences.

BIOMETRICS TECHNOLOGY

Mandated by the USA PATRIOT Act of 2001 and the Enhanced Border Security and Visa Entry Reform Act of 2002, ITL's biometrics program focuses on fingerprint and face recognition testing, multimodal biometrics evaluation and system design, and biometrics standards. In 2004, we produced several reports on evaluations of fingerprint matching systems for the US-VISIT, the new border entry/exit system. (See the Biometrics section of this report.) The website is *http://www.itl.nist.gov/iad/programs.html#BIOMETRICS*.

DIGITAL MEDIA AND MULTIMEDIA TECHNOLOGY

To advance technologies for accessing and using digital- and multi-media, ITL actively participates in multimedia standards development, video retrieval, video analysis and content extraction (VACE), motion image quality (MIQ), optical media testing, visualization and virtual reality for manufacturing, and smart space technologies. In FY 2004, we continued our leadership positions on standards committees such as the Moving Picture Experts Group (MPEG) and Web3D Consortium. We supplemented and continue to maintain the NIST MPEG-7 Interoperability Testbed, with more than 200 members. Our MPEG work provides industry with a profile mechanism for transfer to the marketplace.

ITL works with the Moving Picture Experts Group (MPEG) and government agencies, such as the National Geospatial-Intelligence Agency (NGA), to develop motion image quality (MIQ) metrology. The lack of quality metrology has impeded the development of imaging systems and has inhibited information preservation for compressed imagery. We established a laboratory for image quality studies, and designed and executed verification tests for the MPEG Advanced Video Codec (AVC) and the National Geospatial-Intelligence Agency (NGA) subjective testing. We continued to design and run tests to quantify MIQ and, working with NGA, are developing an MIQ metric.

Video retrieval and analysis is another important focus area. In the VACE project, we collected and provided audio and video domain corpus for use in developing

automatic video extraction algorithms and in building an understanding of content in meetings. In 2004, we developed a draft evaluation specification and annotation guideline for core evaluations of video analysis in collaboration with the University of South Florida, delivered the NIST pilot meeting corpus, and organized the 2004 VACE evaluation workshop.

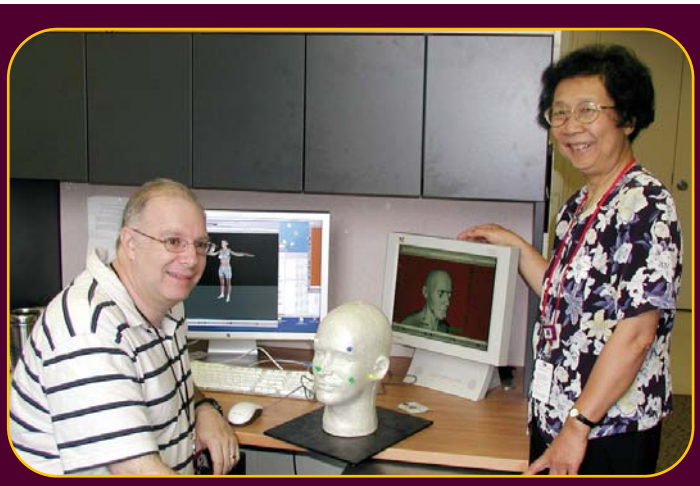
Our visualization and virtual reality for manufacturing project continues to progress. We serve as a member of the Web3D Board of Directors and co-chair the Medical Working Group within the Web3D Consortium, laying the groundwork for medical applications in Web3D.

In the area of digital preservation, we are making contributions to ensure the long-term preservation of digital information. Our projects include a media longevity study, development of standards, and a grading system for archival quality for optical discs, including CDs and DVDs. In 2004, we began a media longevity study in collaboration with the Library of Congress. The results will help government agencies choose the best media for their archival needs. We organized and hosted several meetings of the newly established Government Preservation Working Group, a multi-agency group that will use the longevity results and consult with industry to develop an Archival Grade DVD specification.

In our smart space project, the division established wider cooperative relationships with industry and government programs and aided customer organizations in adoption of our NIST Data Flow system. We developed unique data acquisition hardware (NIST Mk-III Microphone Array), which is now in use at several companies and government projects. We continued to integrate features of the smart space infrastructure into the ITL Meeting Room data acquisition system. Participating in the NIST-wide project in single molecule manipulation and measurement, we helped develop advanced single molecule statistical measurement techniques and published our findings. The website is *http://www.itl.nist.gov/iad/programs.html#Multi*.

INTERACTIVE SYSTEMS TECHNOLOGY

ITL is providing metrics, standards, and test methodologies to improve the usability of interactive systems. Projects include Industry USability Reporting (IUSR), usability and accessibility of voting systems, Novel Intelligence from Massive Data (NIMD), human robot interactions, the Digital Library of Mathematical Functions (DLMF), and accessibility standards.



Sandy Ressler (left) and Qiming Wang discuss standards for 3D graphics for visualizing human body dimensions.

As part of our IUSR project, our Common Industry Format (CIF), adopted as a national standard in 2001, is now in use by several companies for their usability testing. As part of the ITL voting standards effort, IAD performed a study and prepared a report, "Improving the Usability and Accessibility of Voting Systems and Products," which was submitted to Congress by the U.S. Election Assistance Commission in April 2004. We also assisted in the determination of usability experts to serve on the Technical Guidelines Development Committee. (See the Voting Program section of this report.)

For the NIMD project, ITL facilitates the development of user-centered metrics and evaluation methodologies for interactive, intelligent systems and develops metrics for assessing the program by working with researchers in the intelligence community. In FY 2004, we conducted pilot evaluations, updated tools for analyzing data, and assisted in developing future tasks and a roadmap. Our research in human robotic interactions advanced as we conducted data collection and experienced robotic search and rescue events. For the Digital Library of Math Functions (DLMF), we continued to improve 3D interactive visualization of mathematical functions. In the area of IT accessibility, we continued our participation in the INCITS V2 Technical Committee to help develop alternative interfaces for people with disabilities. We also expanded the features of the V2 interface prototype environment using Smart Space technology, progressing toward universal accessibility standards. The website is *http://www.itl.nist.gov/iad/programs.html#Users*. ■

FOUNDATION RESEARCH AREAS

MATHEMATICS

ITL mathematician Dave Gilsinn (right) is working with research engineer Gerry Cheok from the NIST Building and Fire Research Laboratory to demonstrate the use of LADAR technology (laser ranging) for locating equipment on construction sites. He has devised an algorithm to process a LADAR point cloud to determine location and pose of an I-beam in order for a robot crane to acquire it with grippers.

ITL provides technical leadership within NIST in state-of-the-art analytical and computational methods for solving scientific and engineering problems of interest to industry. To do this, we collaborate closely with scientists in the NIST Laboratories on a wide variety of projects. We also develop techniques, tools, and facilities that improve the computational science environment both at NIST and at large. The website is *http://math.nist.gov/mcsd/*.

APPLIED MATHEMATICS

ITL applied mathematicians work in close collaboration with NIST scientists in the development, analysis, and solution of mathematical models of physical phenomena. These collaborations exhibit tremendous variety, with applications ranging from atomic physics to construction engineering.

For example, ITL mathematicians have developed a technique to compute the hard sphere entropy constant, a fundamental quantity from the study of lattice gases in statistical physics used to characterize chemical systems. This computation is equivalent to determining the number of independent sets in a graph, a problem known to be intractable. However, we have developed a stratified sampling approach for estimating this quantity that is highly efficient.

In collaboration with NIST material scientists, we have developed an algorithm for reliably identifying peaks in mass spectroscopy data, a job typically done manually. The technique operates on raw (i.e., noisy) data and is free of adjustable parameters, two features that distinguish it from alternative approaches and make it ideal for metrological applications as well as a fast and reliable method for identifying chemical substances in forensics applications. The algorithm has been embedded in a web-based data analysis service, MassSpectator, now being offered to the public.

We are working with NIST engineers to develop automation methods for construction projects. For example, we are evaluating the use of LADAR (laser ranging) technology for locating equipment and materials on construction sites. In particular, we have developed algorithms for processing a massive collection of noisy LADAR data to determine the location and pose of an I-beam so that a robot crane can position itself to acquire the I-beam with grippers.

HIGH PERFORMANCE COMPUTING

High performance parallel computing is a key enabling technology for modern scientific discovery. We work closely with NIST scientists to develop highly efficient parallel computational models in a wide variety of areas including nanostructures, cement flow, and atomic properties.

For example, we are working with NIST physicists to solve the Schrödinger equation for properties of atoms in optical traps for use in quantum computers. The solution to such problems is extremely challenging, but using novel adaptive grid refinement techniques suitable for parallel computation, we are now able to produce a 48-node eigenstate using a grid with 4.5 million vertices in 35 minutes on a 32-processor PC cluster, a 50-fold speedup over previous attempts.

In FY 2004, we played a leading role in a government-wide effort to revitalize high-end computing. We co-chaired one of the teams that developed *The Federal Plan for High-End Computing*, which lays out a five-year plan to improve how the federal government fosters and exploits computing technologies for the nation's most demanding computational problems.

SCIENTIFIC VISUALIZATION

Visualization is a critical tool for gaining understanding of scientific data, whether the data is the result of physical measurements or output from large-scale computational models. The centerpiece of our efforts in this area is a highly capable immersive visualization laboratory featuring two floor-to-ceiling screens, a floor-based screen, and stereo head-tracked goggles. We are developing an extensive suite of tools that allow us to bring up and interact with scientific data in minutes rather than weeks. Combining such tools with high performance computing, we aim to achieve the goal of science at the speed of thought.

We are applying our tools to the study of the optical properties of nanostructures. Recently, our visualizations of HgS S-orbitals comprising nearly 400,000 atoms allowed NIST physicists to identity a previously unknown state, a significant discovery.

Whitney Austin, a participant in the NIST Summer Undergraduate Research Fellowship program from Jackson State University, worked with ITL computer scientists to develop a calibration facility for the head and wand position tracking sensors used in the ITL Immersive Scientific Visualization facility.

We are also developing new techniques of volume visualization, that is, techniques for visually exploring dense three-dimensional data and applying them to the study of cell growth on polymer scaffolds for applications such as bone implants. To do this, we are working with NIST material scientists who are collecting data using distinct measurement techniques that reflect both functional and structural information. These are combined in the visualization laboratory to produce evocative composite images. See *http://math.nist.gov/mcsd/savg/*.

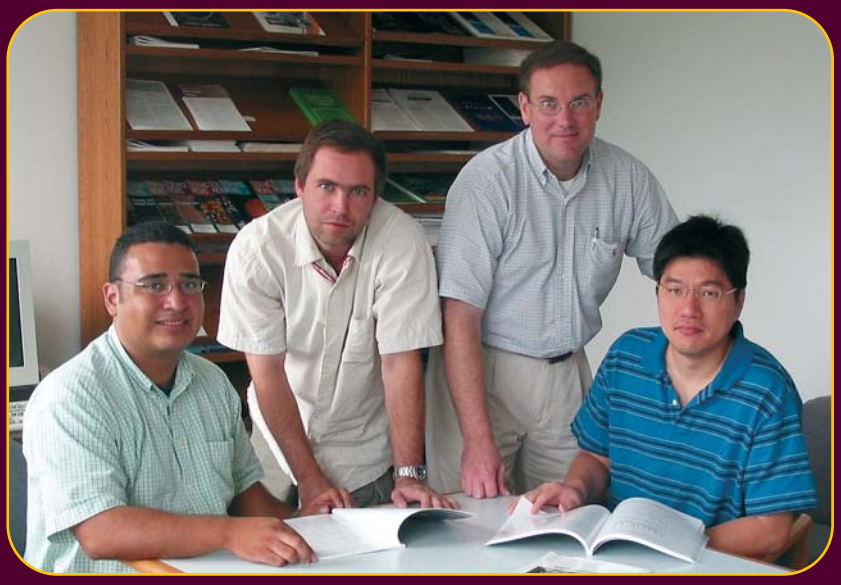
MATHEMATICAL SOFTWARE

To improve the environment for computational research within NIST and the larger scientific community, ITL develops tests and makes available mathematical software and related information services. These span the range from fundamental mathematical components to fully integrated problem-solving environments for particular applications. Active projects include the following:

- Sparse Basic Linear Algebra Subprograms (BLAS): A reference implementation of the interface standard for sparse matrix software
- TNT: Template Numerical Toolkit for numerical linear algebra in C++
- PHAML: Parallel Hierarchical Adaptive Multi-Level solution of partial differential equations
- OOMMF: Object-Oriented Micromagnetic Modeling Framework
- OOF: Object-Oriented Finite Element modeling for materials with complex microstructure

Our web services, including the Guide to Available Mathematical Software (GAMS), saw 4.8 million page downloads from more than 460,000 hosts during the last year. Software download counts during the past year include the following: JAMA (a Java-based linear algebra library) 9,000; TNT 8,800; OOMMF 1,800; and OOF 1,600.

One of our popular products, OOMMF, provides reference software for micromagnetic modeling. It has become an invaluable tool enabling a wealth of significant research in the nanotechnology and magnetics communities. During the last year, 32 papers were published in refereed journals by scientists whose work was enabled by OOMMF. The research spans a wide range of topics such as nanodots, nanorings, and nanowires. More than 120 such papers have appeared since 1999.



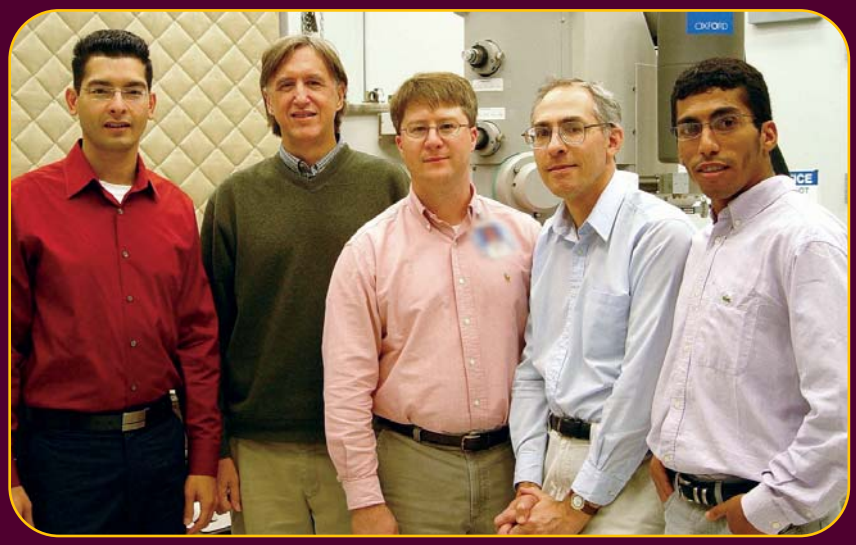
ITL provides opportunities for recent Ph.D.s through the NIST Postdoctoral Associateship Program administered by the National Research Council. Luis Melara (left, seated) and David Cotrell are pursuing research in mathematical models for materials science, while Stephen Bullock and David Song (seated) are studying mathematical problems related to quantum computing and communication.

DIGITAL LIBRARY OF MATHEMATICAL FUNCTIONS

ITL is leading the development of the Digital Library of Mathematical Functions (DLMF), a comprehensive, web-based interactive reference on the special functions of applied mathematics that are heavily used in science and engineering. The DLMF significantly updates and modernizes the NBS *Handbook of Mathematical Functions*, 1964, edited by M. Abramowitz and I. Stegun, which, despite its age, remains a technical bestseller and is among the most widely cited of all mathematical publications. When operational in 2005, the DLMF will provide standardized notations, definitions, and properties for special functions. It will include interactive graphics and a math-aware search system. The core of the DLMF is a mathematics database compiled by some 40 external authors, editors, and validators. In FY 2004, all 38 chapters were accepted, and independent validation was begun. We also completed an XML-based translation system to enable the production of highly interactive MathML-based web pages from author's LaTeX input. See *http://dlmf.nist.gov/.* ■

STATISTICS

ITL is advancing measurement science and technology by formulating and developing statistical theory and methodology for metrology, by collaborating on cutting-edge interdisciplinary science at NIST, and by providing NIST scientists and engineers with state-of-the-art statistical expertise for research. NIST holds a unique international role as the only national metrology institute with a dedicated statistics division. Advances in measurement science and the changing world picture in global economics and international commerce put new emphasis on standards, metrics, and traceability, and on the statistical metrology required by each of these.



Some of the members of the 3D Chemical Imaging at the Nanoscale Competence Project stand in front of an electron microscope in NIST's Advanced Measurement Laboratory. Pictured are (from left) Juan Soto and Don Malec, both of the Statistical Engineering Division (SED); John Henry Scott, Surface and Microanalysis Science Division; Zachary Levine, Electron and Optical Physics Division; and Abderahman Cheniour (SED Guest Researcher).

FUNDAMENTAL METROLOGY

From fundamental scientific research to highly practical work in certifying standard reference materials, the credibility of a measurement or stated value depends on understanding, quantifying, and frequently certifying, its precision – or equivalently, its *uncertainty*. Developing and applying sound statistical methods for determining and calculating uncertainty, for direct and for complex measurement systems, is central to statistical metrology. Dramatic changes in measurement science demand new statistical methodology. Rapid advances in measurement technology and shifts in scientific focus toward the ultra-small (e.g., nanoscience), the ultra-large (e.g., ultra-broad band), and the ultra-complex (e.g., complex failure model for the World Trade Center collapse) all require fundamental advances in statistical metrology.

International metrology and the complex international metrological studies that underpin international commerce and mutual acceptance of standards among international trading partners require specific statistical tools. These international intercomparisons determine degrees of equivalence or magnitudes of systematic offset between metrology institutes in different nations; thus goods that meet the standard in the country of origin may to be purchased with confidence in other nations.

In FY 2004, NIST adopted policy statements *On the Conduct of Key Comparisons* and *On Statistical Principles for Key Comparisons* that originated under ITL leadership. These documents establish requirements for credible, sound statistical analysis of international intermetrology institute studies. Since the number of participating metrology institutes is quite limited for any single international intercomparison, another major ITL contribution is the development of statistical theory and methods to evaluate the equivalence of standards between national metrology institutes that participate in separate, but

Time, as recorded by atomic or mechanical clocks, is still measured with infinitesimal drifts, long-term dependency and jitter; statistical analysis provides the corrections.

linked, international intercomparisons. Additional specific scientific problems, such as instability of traveling artifacts, were also solved, and software created or algorithms made available electronically. In FY 2004, seven statistical papers were published or in press, with five more still in the refereeing process, and thirteen invited presentations given in a variety of venues – professional statistical society, metrology conference, industry, and academia. These new methodologies have now been applied to ten completed international intercomparisons and to three pairs of linked intercomparisons. The website is *http://www.itl.nist.gov/div898/ projects/keycomp.htm*.

In response to the increasingly electronic and/or computational aspect of science, we defined new research areas in FY 2004. In collaboration with industry partners, work began on the fundamental statistical research needed to develop methods for optimal, adaptive, semiautomated, or automated design of experiments. This research is targeted for implementation in chemistry (for theoretically based simulation of an experiment or a calibration, followed by comparative analysis of simulation and bench experiment), for application in materials testing programs (for body armor and shielding gear), and for complex system analysis. A second major new effort focuses on simulation, predictive measurements (virtual measurements), in particular, on the development of principles, practices, and methodology for uncertainty formulation and computation.

STATISTICS FOR PHYSICAL SYSTEMS

Working with NIST scientists and industrial partners, ITL statisticians characterize systems, instruments, and process in mathematical terms. Widespread use of modeling and simulation as a primary tool for scientific investigation is increasing, and measurement systems that incorporate both observed data and computationally generated (virtual) data are becoming prevalent. Simultaneously modeling both small- and large-scale behavior of a system requires integrating statistical approaches into the often multidisciplinary work, *ab initio*.

ITL continues successful collaboration in the modeling of experiments, the design of measurement systems, and the analysis of results from the subatomic particle behavior, the ultra-cold neutron lifetime studies. This series of projects alone produced fourteen publications.

ITL shares a high profile with the Building and Fire Research Laboratory and other laboratories at NIST, in the analysis of the World Trade Center collapse and a reconstruction of the collapse sequence via simulation using multiple linked component simulations. ITL expertise in experimental design and statistical modeling will lead not only to the probable cause analysis but also to a technical basis for improved building structures, eventually in the form of practical guidelines.

In a separate investigation and computational modeling of properties and behavior of structural materials, an ITL statistician and other scientists from the NIST Boulder Laboratories patented their method for determining the residual stress in a structure.

BIOINFORMATICS AND HIGH-D STATISTICS

New research efforts focus on high-dimensional modeling software for high-dimensional data, whether these derive from proteomics or genomics data banks, microarrays, microsensor devices to detect parts per billion contaminants, or single molecule images at the nanoscale. ITL statisticians work in tandem with scientists from NIST's Chemical Science and Technology Laboratory to use statistical modeling, statistical tools, and statistical computation to reduce dimensionality and/or complexity and to extract information as efficiently as possible from the high dimensional data and then to assess the residual

uncertainty. Results obtained so far include latent variable modeling of highly multivariate responses (e.g., genomics data) to develop biomarkers for disease and to elucidate sources of variation, demonstration of successful identification of contaminant(s) via mass spectrometer "signature" at ppb concentrations, and Bayesian 2-D and 3-D reconstruction algorithm for chemical phase of a single molecule. Work to date has led to a new collaboration with the U.S. Food and Drug Administration (FDA) to look simultaneously and in an integrated way at functional performance metrics, the basis for physical standards (NIST), and regulatory standards (FDA) for microarrays, microarray analysis software, and gene expression data and interpretation.

COLLABORATION

As a core contribution to metrology and science at NIST, ITL statisticians provide collaborative research and support for NIST research and measurement services, including the NIST Standard Reference Materials and Calibration Programs. ITL statisticians bring expertise in optimal experimental design, statistical modeling, computational intensive statistics, and data analysis to these collaborative efforts. In FY 2004, over 90 percent of the divisions of the NIST science laboratories sought statistical collaboration from ITL. The writing of entirely new mass calibration software, with customers worldwide, is one example of NIST's influence and ability to improve calibration practices at every level. Another example is the team teaching of the *Advance Mass Measurement Workshop* and the production of CD versions in English and Spanish. Both versions include a central component on basic statistical methods and a second component on uncertainty calculations as part of mass calibration. The website is *http://www.nist.gov/labmetrology.htm*.

EDUCATION

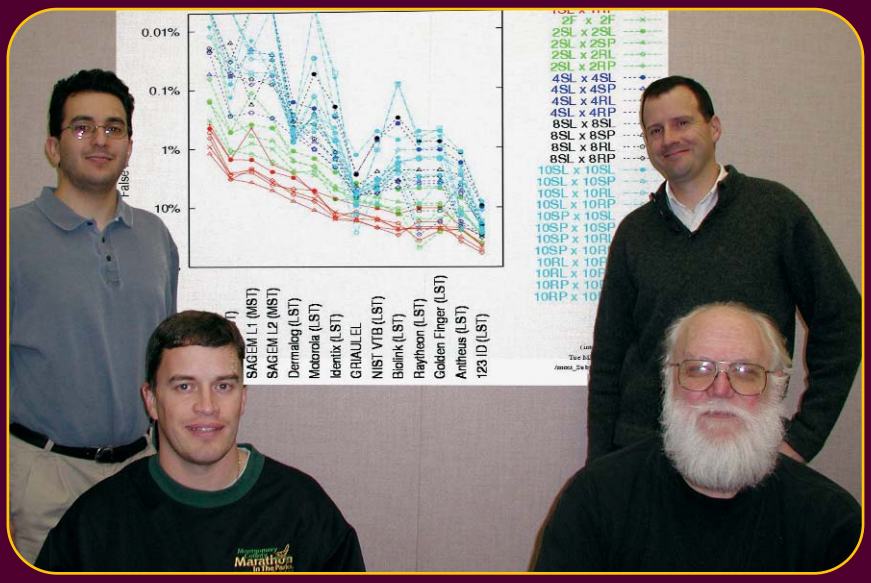
ITL provides education and training that gives NIST researchers the statistical tools necessary to improve the quality of experimental design and data analysis at NIST. With an average of 25-40 NIST scientists per course, ITL statisticians conduct a full series of workshops at both basic and advanced levels, plus short courses in conjunction with metrology conferences or in response to needs of industrial consortia. New courses in FY 2004 included *Data Analysis for Functional Measurements, Estadistica para Experimentos, Statistical Methods for Analyzing Color Differences, Introduction to Nonparametric Regression*, and *e-Handbook and DATAPLOT: An Interactive Demonstration*. We also hosted the international 2004 Spring Research Conference, which was held under the sponsorship of the American Statistical Association, the Institute of Mathematical Statistics, and the Quality and Productivity Society. Additionally, summer students in the Statistical Engineering Division (four in FY 2004) received an education in the form of an apprenticeship in applied statistics, working with mentors on NIST research projects.

(From left) SURF student Van Molino, Andrew Ruhkin, and Stefan Leigh teach Introduction to Markov Chains and Markov Chain Monte Carlo for NIST scientists and engineers.

Made available on the web in 2002, the NIST-SEMATECH *e-Handbook of Engineering Statistics* continues to be a top citation for web searches on "engineering statistics." Now available as a CD, the *e-Handbook* is in its fourth printing, with 6,000 copies already distributed. Newly available on the web, *Case Studies in Statistical Metrology* are designed to acquaint students, scientists, statisticians, and the general public with real examples in statistics for metrology. The websites are *http://www.itl.nist.gov/div898/handbook/index.htm* and *http://www.itl.nist.gov/div898.htm*. ■

SELECTED CROSS-CUTTING THEMES

BIOMETRICS



The Fingerprint Vendor Test Evaluation (FpVTE) NIST team - (clockwise from top left) Ross Micheals, Patrick Grother, Charles Wilson, and Craig Watson - are shown with the two vs. ten fingerprint results which are critical to NIST's USA PATRIOT Act recommendations.

ITL is assisting government and industry in the development and deployment of biometric technologies through evaluation, standards, and research. Mandated by the USA PATRIOT Act of 2001 and the Enhanced Border Security and Visa Entry Reform Act of 2002, our biometrics program centers around fingerprint and face recognition testing, multimodal biometrics evaluation and system design, and biometrics standards.

FINGERPRINT AND FACE RECOGNITION TESTING

ITL has been researching and developing biometric technologies for more than 30 years. In FY 2004, our researchers led the critical evaluations of fingerprint and face recognition technologies that resulted in a report to Congress recommending a dual approach to screen visa applicants and visa holders entering the United States. Co-authored by NIST and the Departments of Justice and State, the report recommends the use of ten fingerprints to positively identify visa applicants and a dual system of two fingerprints and a face image to verify the identities of visa holders at points of entry into the United States. The Department of Homeland Security (DHS) is using the results of this report to design US-VISIT, the new entry/exit system, to better protect U.S. borders.

We continued to provide fingerprint interoperability standards and evaluation technology for the Department of Justice, the FBI, DHS, developers, vendors, and law enforcement organizations. We performed finger verification and identification tests with very large, operational databases. We installed a Cogent system for performing these tests and prepared for 2, 4, 6, and 8-finger testing. We consulted with DHS to help optimize an upgrade path for US-VISIT from 2 plain to more fingerprints.

In FY 2004, we conducted evaluations for Fingerprint Vendor Technology Evaluation (FpVTE) 2003, an independently administered technology evaluation of fingerprint matching, identification, and verification systems for the U.S. Department of Justice. This evaluation was designed to assess the capability of fingerprint systems to meet requirements for both large-scale and small-scale real world applications. FpVTE 2003 consisted of multiple tests performed with combinations of fingers (e.g., single fingers, two index fingers, four to ten fingers) and different types and qualities of operational fingerprints; small, medium, and large-scale tests were conducted using systems provided by 18 participants. The results from the FpVTE will serve as part of NIST's statutory mandate under section 403c of the USA PATRIOT Act to certify those biometric technologies that may be used in US-VISIT. The website is *http://fpvte.nist.gov/*.

In FY 2004, we conducted testing of software development kits (SDK) based on commercial off-the-shelf fingerprint matching systems to evaluate the accuracy of one-to-one matching used in the US-VISIT program. We also evaluated the matching performance for the US-VISIT IDENT systems using flat fingerprints and reported on our studies of plain-to-rolled fingerprint matching using the NIST algorithm testbed. The website is *http://www.itl.nist.gov/iad/894.03/fing/fing.html*.

Face recognition testing is another area of ITL expertise. In FY 2004, we helped launch the new Face Recognition Grand Challenge, an evaluation sponsored by the Intelligence Technology Innovation Center (ITIC), the Technical Support Working Group (TSWG), and the FBI, to explore more complex face recognition systems. Initial designs of experiments were developed for the FY2005 evaluations, including comparison of matching performance of images collected in controlled and uncontrolled indoor environments and 3D imaging. The website is *http://www.itl.nist.gov/iad/894.03/face/face.html*.

MULTIMODAL BIOMETRICS EVALUATION AND SYSTEM DESIGN

We developed a testing methodology and system design for multimodal biometrics. In FY 2004, we developed a prototype for a multimodal biometric system that will provide the infrastructure for collecting multimodal biometric data and for obtaining data about collection biometrics. Data collection will include fingerprints, iris, and facial images for future evaluations. The website is *http://www.itl.nist.gov/iad/894.03/fing/imbe04_rjm.ppt*.

NIST BIOMETRIC STANDARDS PROGRAM

The program's goal is to accelerate the development of high-priority national and international biometric standards in support of accelerating deployments of significantly better, open systems standards-based security solutions meeting users' needs for strong personal authentication. The program is responding to legislative mandates such as the National Technology Transfer and Advancement Act (NTTAA) and, following terrorist attacks in the United States on September 11, 2001, to new legislative requirements, which include the USA PATRIOT Act and the Aviation and Transportation Security Act.

Leadership in National and International Biometric Standard Development Bodies

ITL is a major catalyst of biometric standards development and implementation. Immediately after September 11, 2001, and in close partnership with other U.S. government agencies and industry, we championed the successful establishment of formal national and international biometric consensus standards development bodies (i.e., InterNational Committee for Information Technology Standards (INCITS), Technical Committee M1 – *Biometrics*, and Subcommittee (SC) 37 – *Biometrics* of the ISO/IEC Joint Technical Committee 1). INCITS M1 represents the U.S. in JTC 1 SC 37.

ITL provides the chairperson for INCITS M1 and its Biometric Application Profiles Task Group. We also provide technical editors for three of the M1 projects and a team of experts that actively participate in the development of the M1 standards. During FY 2004, we published NISTIR 6529-A, *Common Biometric Exchange Formats Framework (CBEFF)*, and offered this specification

Elham Tabassi and Karen Marshall discuss the acquisition of fingerprint images in ITL's MBARK Laboratory.

to INCITS for fast track as an ANSI INCITS standard. ITL also initiated the development of an experimental conformance test bed in support of the Biometric Application Programming Interface (BioAPI) specification. JTC 1 SC 37 has a program of work similar to INCITS M1. In addition to providing the SC 37 chairperson, ITL provides the convener of the Biometric Profiles Working Group and technical editors for three of the standards under development. Our biometric experts also participate in SC 37 technical activities. In 2004, INCITS recognized NIST with the INCITS Gene Milligan Award for Effective Committee Management for its leadership and involvement in the development of these national and international standards.

(Clockwise from bottom left) Patrick Grother and Mike McCabe (Information Access Division), Fernando Podio (Computer Security Division), and Mike Hogan (ITL Office of the Director) serve as the key ITL contributors leading the development of the biometrics standards in the INCITS M1 technical committee.

Approval and Adoption of Biometric Standards

During FY 2004, seven standards developed under INCITS M1 were approved as ANSI INCITS standards. Five biometric data interchange format standards and two biometric application profiles were approved: (a) Finger Pattern Based; (b) Finger Minutiae; (c) Iris images; (d) Finger Image-Based; (e) Face Recognition Format; (f) Biometric-Based Verification and Identification of Transportation Workers; and (g) Biometric-Based Personal Identification for Border Management.

Ongoing government programs require conformance to some of the M1 biometric standards. Phase III - Biometric Requirements for the DHS/TSA Transportation Worker Identification Credential Program require, as applicable, the Transportation Workers Biometric profile. The U.S. Department of Defense IT Standards Registry requires the BioAPI and CBEFF. During 2004, two organizations adopted SC 37 standards. The International Civil Aviation Organization included requirements for the machine-readable travel documents requirements for the facial recognition data format; the fingerprint data formats, and the iris data format. CBEFF is also a requirement. The International Labour Office of the United Nations also requires some of the SC 37 standards for their use in a Seafarers' ID Card: finger minutiae and finger image data interchange formats, BioAPI, and CBEFF.

ITL's Biometrics Resource Center website is *http://www.nist.gov/biometrics.*

SELECTED CROSS-CUTTING THEMES

CRITICAL INFRASTRUCTURE PROTECTION

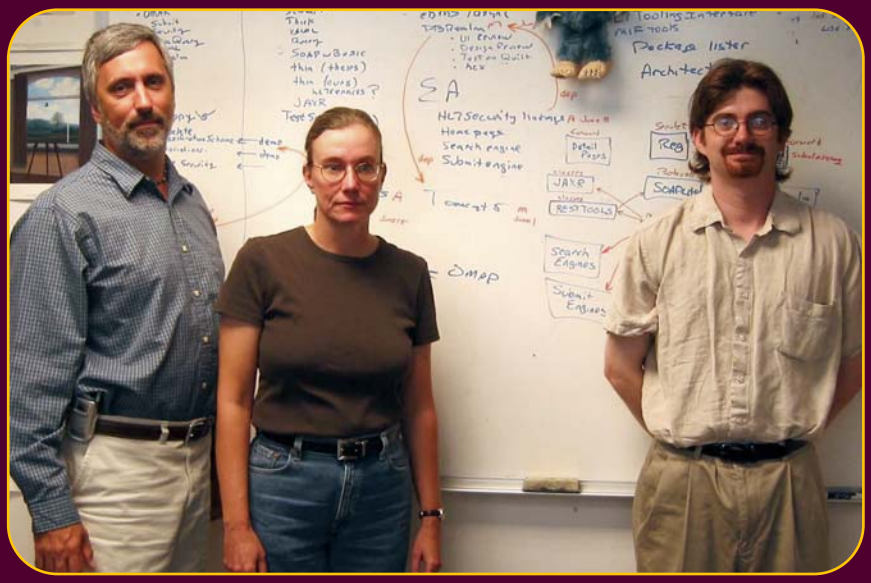
Securing the information technology (IT) systems of our nation's critical infrastructures is one of the highest priorities of the U.S. government. Natural disasters, extensive and prolonged power outages, the increasing incidence of Internet hackers and viruses, the terrorist attacks of September 11, 2001, and the ongoing war on terror, all contribute to a sense of urgency about the security and reliability of the nation's physical infrastructures and the information systems on which they rely. Infrastructures such as communications systems, electricity and other energy services, financial services, water delivery systems, and transportation networks have become increasingly automated and interlinked. This creates new vulnerabilities such as equipment and network failures, human error, weather and other natural causes, and physical and cyber attacks.

ITL focuses on IT security standards and testing to help ensure the security of our nation's critical infrastructures.

Consistent with our mission and long-standing IT security responsibilities, ITL focuses on security standards, guidance, metrics, and testing to help protect the information systems of our nation's critical infrastructures. We support federal departments and agencies under the Federal Information Security Management Act (FISMA) of 2002 and other legislation that assigns to NIST responsibility to develop security standards and guidelines for sensitive, unclassified federal systems. Through the development of standards and testing programs, we are helping IT developers and vendors to build products that better protect information systems and improve security for all citizens. (See the Security section of this report.) These improved products, in turn, enhance the security of the communications and information processing backbone of our nation's critical infrastructures. ■

SELECTED CROSS-CUTTING THEMES

HEALTHCARE



Bill Majurski, Mary Laamanen, and Andrew McCaffrey improve timely access to patient clinical information through their clinical document registry implementation, a focal point for integrating healthcare environments.

ITL and the healthcare community are working together to successfully implement current healthcare standards and to achieve interoperability in using them. Appropriate standards for healthcare information and systems provide the cornerstone to achieving a healthcare infrastructure. Our healthcare initiative (*http://www.nist.gov/ehealth*) seeks to advance healthcare information standards that are complete and testable and to provide the needed conformance tests, interoperability tools, and techniques. In support of the NIST Healthcare Strategic Focus Area, we concentrate our resources in four focus areas.

Focus Area 1. Messaging standards and technologies that move clinical information from system to system. ITL is collaborating with Health Level Seven (HL7), an American National Standards Institute (ANSI)-accredited standards organization, to improve the deployment of HL7 standards for moving patient information between healthcare applications. We are developing a test tool that will determine if an HL7 implementation is conformant with respect to the HL7 standard, which will ensure two healthcare systems to be interoperable. We also developed an HL7 Experimental Registry to further the correctness of HL7 message definitions and their availability.

To address the need for interoperability among ventilators, monitors, IVs, and support devices in an intensive care unit, the Institute of Electrical and Electronics Engineers (IEEE) Medical Device Communications Working Group (IEEE 1073 WG) developed a set of standards for medical device communications. Implementations of these standards will enable clinicians to link patient-connected medical devices to a computer network, permitting comprehensive data capture from monitoring devices. We are collaborating with the IEEE 1073 WG to develop conformance tests and associated tools to ensure that critical devices properly implement the medical device standards.

To advance the integration of many clinical, administrative, and IT standards, ITL provides prototypes and reference implementations of profiles created by integrating emerging healthcare and IT standards. Under our leadership, new profiles are being developed based on these implementations. The web-based prototypes and reference implementations allow full integration of standards necessary to build a standards-based healthcare environment. A myriad of vendors seeking to develop healthcare products use this environment to determine interoperability with other products.

Focus Area 2. Electronic health record standards that provide clinicians with all relevant patient information. In order for clinicians to access all relevant medical information regarding a specific patient, a standard defining the structure and context of an electronic health record (EHR) must be established and implemented. HL7 created the EHR System Functional Model: Draft Standard for Trial Use, which defines the functions necessary for an EHR system. ITL is defining conformance language and criteria necessary for conformance and certification-related activities, thus leading the conformance effort as it moves from conformance definition to test definition and development. Further, private industry certification bodies use our expertise to develop EHR-product certification programs.

Focus Area 3. Guidelines and technologies that promote a secure and reliable healthcare environment. Medical environment requirements have life or death implications when data is lost, corrupted, or delayed. As hospital beds and acute-care rooms become more 'plugged-in,' the move toward a wireless environment becomes more attractive. The IEEE 1073 WG is currently defining standards for medical device communication focusing on wireless technologies that are adequate to the clinical domain and the patient's bedside. ITL is collaborating with the IEEE 1073 WG to focus on the scalability issues and the need to support multiple communicating devices over a wireless network within a patient's hospital room.

Healthcare accreditation guidance is another area of interest. NIST in conjunction with URAC (not an acronym) and the Workgroup of EDI (WEDI) sponsors the NIST/URAC/WEDI Healthcare Security Workgroup. The group brings together key stakeholders from the public and private sectors to facilitate communication and consensus on best practices for information security in healthcare. The group draws heavily upon information technology (IT) security standards and guidelines developed by ITL. Ultimately, these best practices will be integrated into accreditation criteria used by hospitals and other healthcare facilities.

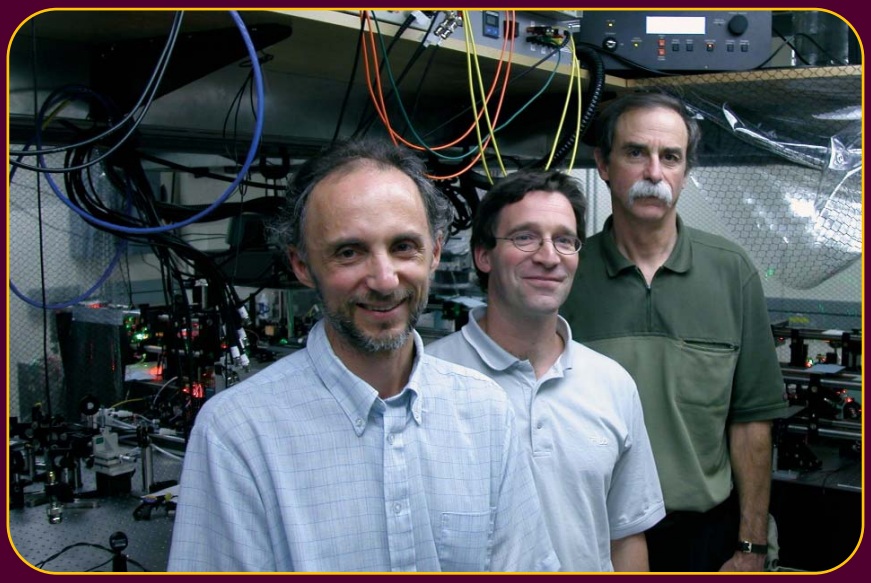
Focus Area 4. Awareness efforts that focus on both security and interoperability. Telemedicine allows patients to gain access to healthcare professionals electronically regardless of their location, providing faster, more affordable healthcare services. ITL worked with the American Telemedicine Association to define a portfolio of standards and guidelines to provide ocular care through telecommunications technology. The process by which this diabetic retinopathy portfolio of standards was developed will next be applied to electrocardiogram image capture, storage, rendering, and management.

To improve the integration and interoperability of IT standards and tools for the exchange of healthcare information, ITL established a repository of healthcare standards and implementation information that can be used by all groups and stakeholders in developing and applying healthcare standards. Our Healthcare Standards Landscape is a web-based framework for building and maintaining a repository of information on relevant healthcare standards, initiatives, organizations, and implementation efforts that enable developers and stakeholders to readily obtain needed information that can improve standards development, coordination, and the realization of more compatible standards and tools.

A final project assists the healthcare community in understanding and implementing the Security Rule under the Healthcare Insurance Portability and Accountability Act (HIPAA). This legislation directs organizations that create, store, and process healthcare information to operate in a manner that keeps healthcare information secure and maintains patient privacy. To assist readers in complying with the legislation, we developed NIST Special Publication 800-66, *An Introductory Resource Guide for Implementing the HIPAA Security Rule* (DRAFT), available at *http://csrc.nist.gov/publications/nistpubs/index.html.* ■

SELECTED CROSS-CUTTING THEMES

QUANTUM INFORMATION



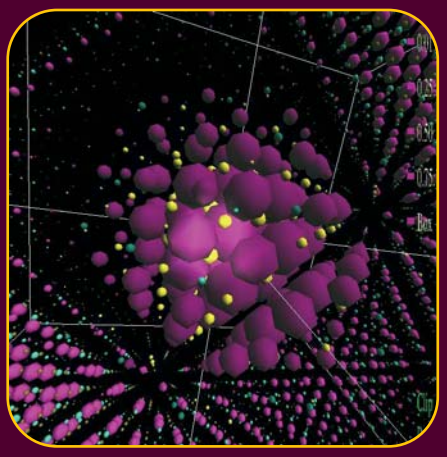
ITL mathematician Emanuel Knill (left) collaborated with NIST physicists Dietrich Leibfried and team leader David Wineland to develop the first demonstration of quantum teleportation in atoms recently published in Nature (M.D. Barrett et al., Nature v429 p737 2004). Teleportation is expected to be a critical operation in future quantum computers.

The recent marriage of quantum physics and computer science, two of the great scientific revolutions of the 20th century, has the potential to radically transform future information technologies. ITL is participating in the NIST Quantum Information program, which aims to develop a measurement and standards infrastructure to enable future information systems based on the principles of quantum physics. Working in collaboration with the NIST Physics and Electronics and Electrical Engineering Laboratories, ITL's goals are to understand the potential for quantum information to revolutionize information science, to develop and test secure, commercial-grade quantum communications systems and protocols, and to develop architectures and algorithms to enable the engineering and testing of future quantum computer systems. ITL research in this area is supported in part by the Defense Advanced Research Program Agency and the NIST Competence Program. Four of ITL's divisions participate in two broad program areas.

QUANTUM COMMUNICATIONS

The laws of quantum physics can be exploited to provide a perfectly secure channel for the exchange of cryptographic keys. NIST has developed a testbed for the demonstration and measurement of such technologies. The testbed is based on a free-space optical link between two buildings on the NIST campus. Bits of cryptographic key are transmitted using a beam of single polarized photons (the quantum channel). A second (classical) channel is also needed to implement the B92 key distribution protocol. The properties of quantum physics can be exploited to detect eavesdropping on the quantum channel, a critical property missing in classical systems. This year we demonstrated the exchange of sifted quantum cryptographic key at rates of up to 3.5 Mbps, more than two orders of magnitude faster than previously reported results. To achieve these rates, the system runs synchronously, with clock recovery techniques on the classical channel at 1.25 Gbps enabled by special-purpose high-speed communication boards. Novel techniques of forward error correction and privacy amplification are then used to complete the establishment of cryptographic keys at the two ends of the communication link. When these are applied we obtain net key generation rates of about 1 Mbps. Such high-speed real-time key generation can be used to enable one-time pads, the only unconditionally secure method of data encryption. Current work is focused on increasing key exchange rates and on exploring the potential for multi-node network operations.

In other work, we have developed two new cryptographic key distribution schemes based on swapping quantum entanglement. Using two Bell states, two bits of secret key can be shared between two distant parties that play symmetric and equal roles. The protocols have been shown to be robust against common eavesdropping attacks. Finally, we have also extended and refined our proposed protocols for authentication using quantum resources to provide detection of a compromised server.



ITL staff are working with the NIST Physics Laboratory to enable simulation and visualization of optical properties of complex nanostructures. Structures with more than 370,000 atoms have been simulated. This image shows the structure of a quantum dot.

ARCHITECTURE AND ALGORITHMS FOR QUANTUM COMPUTERS

This year we completed a significant analysis of fault tolerance thresholds for quantum computing which indicate that in some cases errors may be tolerable at much higher rates than previously thought possible. In particular, we proved that if all errors are detected, scalable quantum computation with error rates well above 10% per gate is possible, at least in principle. As part of this work, we introduced the method of teleported error correction to simplify fault tolerant constructions. Applying it to general independent errors, we have found strong evidence that error rates well above 1% per gate are tolerable. We expect that resource overheads to cope with such error rates may be small enough to be realizable with foreseeable technology. The analysis has implications for proposals such as linear optics quantum computation.

We also worked very closely with the NIST Physics Laboratory to realize the first experiment in which quantum states were reliably "teleported" between atoms. Previous experiments had only demonstrated teleportation in optical systems or nuclear magnetic resonance systems. The demonstration is important because it incorporated most of the techniques needed for scalable quantum information processing in an ion trap system. The work was reported in the June 17, 2004, issue of *Nature*.

Another important problem is the mapping of quantum computations onto quantum computers; this is the problem of quantum circuit synthesis. Working with colleagues at the University of Michigan, we have developed a highly practical approach to solving this problem. Our work is based on a new universal quantum circuit capable of implementing any unitary operator (mathematically, all quantum computations may be represented as operators of this type). The circuit has a top-down structure that concentrates components on the less significant qubits, and the parameters for a given computation may be determined using standard matrix analysis software. A theoretical analysis shows that the universal circuit is nearly optimal, that is, the number of gates for any given computation may be improved by at most a factor of two. The circuit adapts well to architectures in which only nearest-neighbor interactions are possible.

In 1985, David Deutsch, a quantum information pioneer from Oxford University, suggested a simple algorithm which first demonstrated a case in which a quantum computer could outperform a classical one. We have developed a generalization to Deutsch's algorithm that distinguishes between so-called concentrated maps and one-to-one finite integer functions in a constant number of samples (with high probability). This shows that quantum out-performance is somewhat more robust in this classic example.

While routine quantum computation remains a distant reality, we hope that our research work will help provide a clearer pathway from physics experiments to practical computation systems. The web page is *http://math.nist.gov/quantum/*. ■

SELECTED CROSS-CUTTING THEMES

VOTING PROGRAM

As project leader of the NIST Voting Systems Standards effort, Allan Eustis gave welcoming remarks as chair of the 1st NIST Symposium on Building Trust & Confidence in Voting Systems, held on December 10-11, 2003.

Mandated by the Help America Vote Act (HAVA) of 2002, ITL is working with the U.S. Election Assistance Commission (EAC) to enhance the capacity and performance of the nation's voting systems through the development and promotion of standards, measures, and technology. Our program consists primarily of intramural R&D and conformity assessment efforts and outreach to the election community. Additionally, we support the EAC's Technical Guidelines Development Committee (TGDC), a group of 15 members that is chaired by the NIST Director. The HAVA-mandated duties of the TGDC include the gathering and analysis of data and information related to the security of computers, human factors, voter privacy, and methods to detect and prevent fraud. As leader of the NIST Voting Systems Standards project, ITL leads a diverse group across NIST including personnel from four divisions in ITL, the Manufacturing Engineering Laboratory, Technology Services, and the Office of the Director. Our election community customers include concerned citizens, the disabled, states and counties, voting equipment vendors, academic researchers, and independent testing laboratories. The website is *http://vote.nist.gov*.

On December 10-11, 2003, ITL hosted a groundbreaking voting standards symposium. Over 300 computer scientists, vendors, voting rights activists, Secretaries of State, and local election officials participated in NIST's *First Symposium on Building Trust and Confidence in Voting Systems*. Participants discussed and debated challenging computer security and usability issues related to HAVA and the role NIST would play in the law's implementation. ITL panel moderators briefed the attendees on relevant expertise available to the election community to improve public trust and confidence in voting systems.

On March 22, 2004, ITL facilitated the first meeting of the EAC. The commission was created under the Help America Vote Act to recommend new voluntary voting system guidelines to state and local governments. The NIST Director chairs the Technical Guidelines Development Committee, which will research and recommend new guidelines to the EAC. ITL provides technical support to the committee, notably intramural R&D in the areas of usability, accuracy, security, accessibility, and integrity of voting systems, protection of voter privacy, and remote access voting.

On April 30, 2004, the EAC submitted to both Houses of Congress a human factors report, NIST Special Publication 500-256, *Improving Usability and Accessibility of Voting Systems and Products*. ITL led the team that researched and wrote the report to fulfill a requirement of HAVA. The report contains ten recommendations that, if followed, should measurably improve the usability and accessibility of voting products and systems. The lead author reviewed the report's findings during testimony on May 5th at an EAC public hearing on electronic voting systems.

According to the report, the single most critical need is a set of usability standards for voting systems that are performance-based and support objective measures and associated conformance test procedures that can be used for the certification and qualification of voting products and systems.

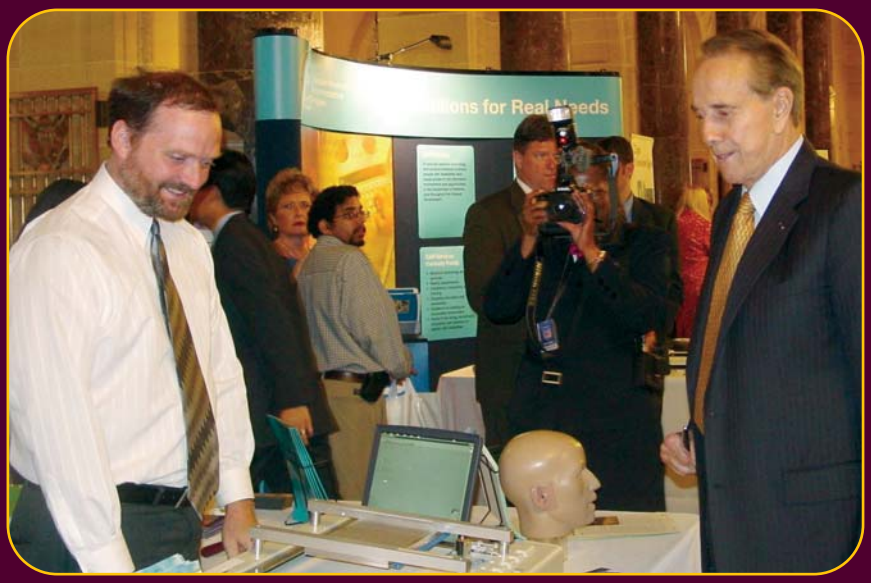
Another focus of ITL's technical assistance program is the security of voting software and conformity assessment. The EAC chairman identified our National Software Reference Library (NSRL) as one part of a five-point strategy to improve electronic voting security for the November 2004 presidential election and beyond. The chairman stated that the EAC should invite every voting software vendor to submit their certified software to our NSRL to facilitate the tracking of software version usage. NSRL is designed to collect software from various sources and incorporate file profiles computed from this software into a Reference Data Set (RDS) of information. Law enforcement, government, and industry can use the RDS to review files on a computer by matching file profiles in the RDS. The NSRL was built to meet the needs of the law enforcement community for rigorously verified data that can meet the exacting requirements of the criminal justice system.

As its chairman, the NIST Director gaveled the first meeting of the Technical Guidelines Development Committee to order on July 9, 2004. HAVA charges the committee with the recommendation of new voluntary voting system standards to the EAC. ITL scientists briefed the committee on writing quality specifications, the capabilities of the NSRL and the potential for its use by election officials to ensure voting software integrity, the findings of NIST Special Publication 500-256, *Improving Usability and Accessibility of Voting Systems and Products*, and current interagency security testing programs of potential value to the election community.

On September 20-22, 2004, ITL hosted public hearings of the Technical Guidelines Development Committee to collect data and information from stakeholders in the election community. Over 80 people attended one or more days of the public hearings including congressional committee staffers, election administrators, the press, and the public. Panels of experts offered testimony and answered TGDC members' questions on HAVA-related issues including security, transparency, human factors, privacy, and core standards requirements and testing of voting systems. At the conclusion of each day, members of the public testified on several issues including new voting technologies and improving voting systems for use by the disabled. Testimony from the hearings has been posted at *http://www.vote.nist.gov/HearingsandTranscripts.htm.* ■

Computer scientist Sharon Laskowski testified at the first public hearing of the Election Assistance Commission (EAC) on May 5, 2004. In her remarks, she highlighted the findings from the NIST Human Factors Report: Improving the Usability and Accessibility of Voting Systems and Products. *Laskowski was the lead author of this report to Congress.*

INDUSTRY AND INTERNATIONAL INTERACTIONS



Project leader John Roberts, Information Access Division, demonstrated the NIST Refreshable Tactile Graphic Display, developed by his team, at the NIST booth in the joint Department of Commerce (DoC)/Department of Education Assistive Technology Exhibit and Policy Forum. Held on July 27, 2004, at DoC headquarters, the forum commemorated the 14th anniversary of the Americans with Disabilities Act. Distinguished visitors to the NIST booth included the Honorable Bob Dole.

ITL's research, measurement, and standards programs are greatly enhanced by our interactions with partners in industry, academia, government, and standards developers, both at home and abroad. Our program of work is enriched by our participation in many consortia and industry interest groups, including the following:

AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI)

ANSI has served as administrator and coordinator of the U.S. private sector voluntary standardization system for 80 years. Thomas Rhodes and Lisa Carnahan serve on the ANSI Healthcare Informatics Standards Board (HISB), while Fernando Podio serves on the Homeland Security Standards Panel Steering Committee. NIST/ITL is an ANSI-accredited standards developer. Michael McCabe is the contact for ANSI/NIST-ITL 1/2000, *Data Format for the Interchange of Fingerprint, Facial, & SMT Information.*

ASTM

ASTM (American Society for Testing and Materials) is a nonprofit organization that provides a forum for producers, users, ultimate consumers, and those having a general interest (representatives of government and academia) to meet on common ground and write standards for materials, products,

systems, and services. Through the participation of Nien-Fan Zhang in Technical Committee E-11, ITL promotes quality in statistics. Gordon Lyon participates in Technical Committee E-31, International Healthcare Informatics, Continuity of Care Record.

ITL has developed fast and effective image deblurring methods that do not require prior knowledge of the blurring kernel. This year ITL's APEX method was adapted for use in color imagery. Here an original Hubble telescope image of the Orion reflection nebula NGC 1999 (left) is sharpened by the APEX method (right).

BIOMETRIC APPLICATION PROGRAMMING INTERFACE (BioAPI) CONSORTIUM

The BioAPI Consortium is an international organization of over 100 members including IT organizations, biometric vendors, and users. The consortium developed the BioAPI specification v1.1, ANSI/INCITS 358. Fernando Podio serves on the Steering Committee and chairs the BioAPI External Liaisons Working Group. As an open systems specification, the BioAPI is intended for use across a broad spectrum of computing environments to ensure cross-platform support.

BIOMETRIC CONSORTIUM (BC)

The NIST/National Security Agency BC serves as the federal government's focal point for research, development, test, evaluation, and application of biometric-based personal identification/verification technology. It currently consists of over 1,000 members representing over 60 government agencies, industry, and academia. The BC holds an annual conference and technical workshops. The conference held September 20–22, 2004, in Crystal City, Virginia, was one of the largest conferences worldwide dedicated solely to biometrics. Fernando Podio co-chairs the Biometric Consortium as well as the Biometric Interoperability, Performance, and Assurance Working Group.

CROSS INDUSTRY WORKING TEAM (XIWT)

The XIWT is a multi-industry coalition of IT companies that attempts to identify common issues and concerns in IT strategic directions and policy matters. ITL's participation assists in this process by providing technical guidance that bridges the gap between the research, standardization, and policy communities. Doug Montgomery represents NIST on the executive committee.

DVD ASSOCIATION (DVDA)

The DVDA represents standards developers, software developers, disc and electronics manufacturers, government agencies, and content developers of DVD and associated technologies. Oliver Slattery and Fred Byers represent ITL. Through our representation, we facilitate standards, interoperability, and compatibility for writable DVD media, disc drives, and consumer electronic players.

eGOV CONSOLIDATED HEALTH INFORMATICS

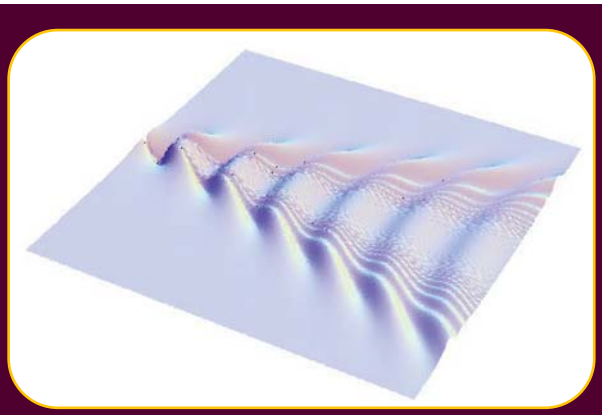
The Consolidated Health Informatics Initiative is the healthcare component of the Administration's eGov initiative. The committee facilitates the adoption of a common coding system for patient medical information, so that federal agencies will be able to exchange information without having to translate it into a new system. Tom Rhodes represents ITL on the committee. Through our participation, ITL is helping to standardize federal clinical health information.

ELECTIONS ASSISTANCE COMMISSION (EAC)

Mandated by the Help America Vote Act (HAVA) of 2002, NIST supports the EAC as chair of the Technical Guidelines Development Committee (TGDC). The TGDC makes recommendations to the EAC on voluntary standards and guidelines related to voting machines. ITL is coordinating the agency's HAVA efforts through its expertise in areas such as computer security and usability. Allan Eustis is the project leader for the voting systems standards project. Sharon Laskowski, Barbara Guttman, Annabelle Lee, Nelson Hastings, and John Wack contribute to the project.

FORUM ON PRIVACY AND SECURITY IN HEALTHCARE (FPSH)

Sponsored by the National Information Assurance Partnership (NIAP, a joint National Institute of Standards and Technology and National Security Agency initiative) and the Healthcare Open Systems and Trial (HOST), the FPSH is incorporated as a nonprofit charitable organization consisting of participating members from approximately 50 healthcare organizations. Arnold Johnson represents ITL, which with support from the NIST Advanced Technology Program (ATP) and NIAP, is developing guidance material and reference Common Criteria (CC)-based profiles to assist, demonstrate, and educate the healthcare community in specifying Protection Profile security requirements using the ISO/IEC 15408 CC standard.



This computed image of the wake behind a boat, known as Kelvin's ship wave pattern, is an application of the Airy function of applied mathematics. Properties of such functions will be cataloged in ITL's Digital Library of Mathematical Functions.

HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, INTEGRATING THE HEALTHCARE ENVIRONMENT (HIMSS/IHE)

HIMSS is the healthcare industry's membership organization exclusively focused on providing leadership for the optimal use of healthcare information technology and management systems for the betterment of human health. Founded in 1961 with offices in Chicago, Washington D.C., and other locations across the country, HIMSS represents more than 14,000 individual members and some 220 member corporations that employ more than 1 million people. HIMSS frames and leads healthcare public policy and industry practices through its advocacy, educational, and professional development initiatives designed to promote information and management systems' contributions to ensuring quality patient care. William Majurski represents ITL in the organization.

HEALTH LEVEL 7 (HL7)

HL7 is an ANSI-accredited standards developing organization that provides standards for the exchange, management, and integration of data to support clinical patient care and the management, delivery, and evaluation of healthcare services. Specifically, HL7 seeks to create flexible, cost-effective approaches, standards, guidelines, methodologies, and related services for interoperability between healthcare information systems. Lisa Carnahan, Robert Snelick, and Leonard Gallagher represent ITL in the HL7 Conformance Special Interest Group (SIG). Carnahan and Gallagher also serve on the HL7 Modeling and Methodology Technical Committee. Gordon Lyon and Anthony Cincotta participate in the Electronic Health Records activity, and William Majurski contributes to the HL7 Templates SIG. Our expertise advances the interoperability of systems delivering healthcare services.

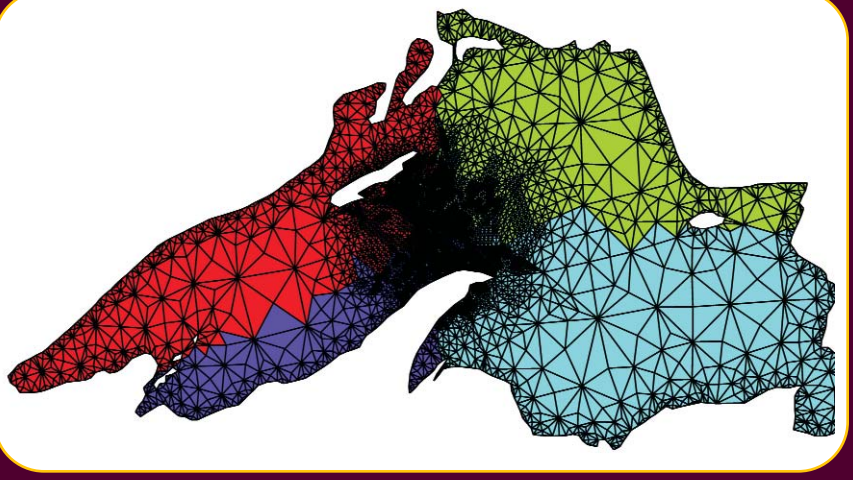
HIGH DENSITY STORAGE ASSOCIATION (HDSA)

The HDSA has a well-defined charter to focus on automated, storage-centric technologies, known as jukebox or library storage, and acts as a centralized communicator among the industry, resellers, and users. The group identifies interoperability, connectivity, and compatibility issues and develops specifications to

enhance the storage infrastructure. Oliver Slattery represents ITL, which provides a neutral platform to perform testing and development so the industry can improve the interoperability and performance of products for high-density data storage.

INDUSTRY USABILITY REPORTING PROJECT (IUSR)

This NIST/industry collaboration resulted in the development of a Common Industry Format (CIF) for sharing usability data with consumer organizations. The reporting format was adopted as a national standard (ANSI / INCITS 354) in November 2001. Jean Scholtz, Sharon Laskowski, and Emile Morse lead the ITL effort and facilitate the international standardization of CIF.



ITL's PHAML software for the parallel adaptive solution of partial differential equations has recently been extended to deal with complicated spatial domains. This image shows an adaptive grid computed by PHAML for Lake Superior.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

The world's largest technical professional society, IEEE focuses on advancing the theory and practice of electrical, electronics and computer engineering, and computer science. Sharon Laskowski participates in P2001, Web Best Practices Working Group (WG). Sheila Frankel contributes to IEEE 802.11i, Task Group I: WG on Wireless Local Area Networks (Security). David Cypher, Robert Van Dyck, and Nada Golmie participate in IEEE 802.15, WG for Wireless Personal Area Networks. Mary Brady and Richard Rivello participate in IEEE 1073, Medical Device Communications. Larry Reeker participates in IEEE P1600.1, Standard Upper Ontology WG, and represents ITL on the Industrial Advisory Board of the Software Engineering Body of Knowledge (SWEBOK) project, which seeks to identify the body of knowledge of software engineering and to provide suitable access to that knowledge. Stuart Katzke and Alicia Clay participate in IEEE P1700, Information Assurance: Standard for Information System Security Assurance Architecture. Through these contributions, ITL advances information science in a broad spectrum of IT areas.

INTERNATIONAL COMMITTEE FOR INFORMATION TECHNOLOGY STANDARDS (INCITS)

INCITS's mission is to produce market-driven, voluntary consensus standards in a wide range of IT areas. Michael Hogan and Alicia Clay serve on the INCITS Executive Board and Standards Policy Board. Teresa Schwarzhoff and Jim Dray participate in TC B10, Identification Cards and Related Devices. Mike Rubinfeld chairs and Mike McCabe and Wo Chang serve on TC L3, Coding of Audio, Picture, Multimedia and Hypermedia Information. Chang and Rubinfeld also participate in TG L3.1, MPEG Development Activity. Rubinfeld, McCabe, and Chang contribute to TG L3.2, Still Image Coding. Fernando Podio chairs and McCabe, Hogan, and Patrick Grother participate in TC M1, Biometrics. Podio and Hogan contribute to TG M1.2, Biometric Technical Interfaces; McCabe and Hogan are also on TG M1.3, Biometric Data Interchange Formats; Podio chairs and Hogan participates in TG M1.4, Biometric Application Profiles; Grother and Hogan are on TG M1.5, Biometric Performance Testing and Reporting; David Cooper participates in TC T3, Open Distributed Processing; Alicia Clay and Randall Easter serve on TC T4, IT Security Techniques; and Sharon Laskowski and Charles Sheppard represent ITL on TC V2, IT Access Interfaces. Through these interactions, we contribute our expertise to the development of IT industry standards.

INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING (IFIP)

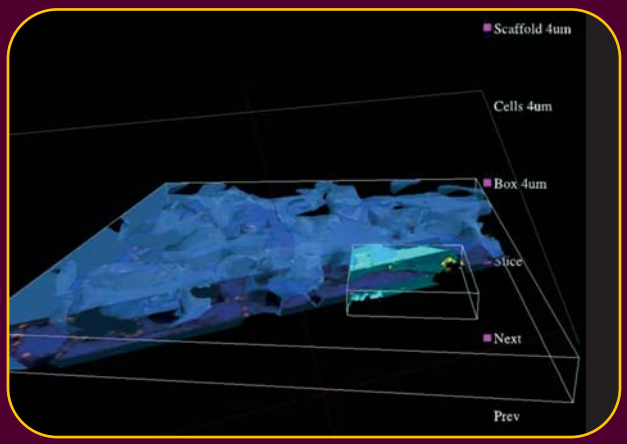
Ronald Boisvert chairs the IFIP Working Group 2.5, Numerical Software, which strives to improve the quality of numerical computation by promoting international cooperation in the development of languages, guidelines, tools, and standards for numerical software.

INTERNATIONAL MATHEMATICAL UNION (IMU)

IMU is an international nongovernmental and nonprofit scientific organization, with the purpose of promoting international cooperation in mathematics. Daniel Lozier serves on the Technical Advisory Board of the Committee for Electronic Information and Communication.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)

The ISO is a worldwide federation of national standards bodies from some 140 countries, one from each country. Nien-Fan Zhang serves on the Committee on Reference Materials (REMCO) WG1 for ISO Guide 35. Zhang and Nell Sedransk participate in the management group for ISO TC 69, Statistical Methods. Our contributions facilitate the development of international agreements that are published as International Standards.



ITL is working with scientists from the NIST Materials Science and Engineering Laboratory to enable immersive visualization of data from experiments. Here data from two types of microscopes (optical coherence tomography and confocal flourescence microscopy) are combined to visualize cells growing on a polymer scaffold.

INTERNET ENGINEERING TASK FORCE (IETF)

ITL contributes to the technical development of the Internet through participation in the IETF, which is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. Doug Montgomery, Scott Rose, and Sheila Frankel participate in the Internet Area; David Griffith participates in the SUB-IP Area; Mark Carson, Leonard Miller, Nader Moayeri, Luke KleinBerndt and Montgomery participate in the Routing Area; Montgomery, Okhee Kim, Frankel, Nelson Hastings, and Tim Polk participate in the Security Area; Polk also chairs the PKI Using X.509 Working Group; and Montgomery and Mudumbai Ranganathan participate in the Transport Area.

INTEROPERABLE MESSAGE PASSING INTERFACE (IMPI)

ITL actively participates in the development of standards and conformance testing for IMPI. William George, John Hagedorn, and Judy Devaney represent ITL; our contributions benefit industries that use a parallel code across different vendor systems, including the embedded computing community.

MICROMAGNETIC MODELING ACTIVITY GROUP

The Micromagnetic Modeling Activity Group is an organization of industrial, government, and academic researchers investigating fundamental issues in micromagnetic modeling through the establishment of standard problems for testing micromagnetic simulation software and the development of a public domain reference implementation of micromagnetic simulation software. Michael Donahue and Donald Porter represent ITL on the steering committee.

MOTION IMAGERY STANDARDS BOARD

The mission of the Motion Imagery Standards Board is to ensure the development, application, and implementation of standards that maintain interoperability and quality for video imagery, associated metadata, audio, and other related systems in the Department of Defense/Intelligence Community/U.S. Imagery Geospatial Information System. Wo Chang and Charles Fenimore participate for ITL.

MOVING PICTURES EXPERTS GROUP (MPEG) INDUSTRY FORUM

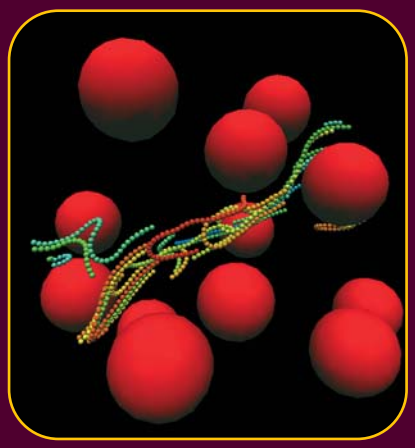
MPEG is a working group of ISO/IEC in charge of the development of standards for coded representation of digital audio and video. The MPEG Industry Forum is a nonprofit organization that strives to further the adoption of MPEG standards, by establishing them as well accepted and widely used standards among creators of content, developers, manufacturers, providers of services, and users. Wo Chang represents ITL.

NATIONAL FILE FORMAT ADVISORY PANEL

The National File Format Advisory Panel, which reports to the U.S. Secretary of Education, has been working on the National Instructional Materials Accessibility Standard (NIMAS). This standard will specify the file format to be used by publishers of textbooks and other instructional materials, in order to maximize accessibility to the material. Examples of accessibility issues include formatting the textbook files so they can be easily translated into Braille, correlating text and speech forms of material, and providing alternate presentations formats, such as those for students with learning disabilities. John Roberts represents ITL on the panel.

NATIONAL PUBLIC SAFETY TELECOMMUNICATIONS COUNCIL (NPSTC)

Formed May 1, 1997, the NPSTC is a federation of associations representing public safety telecommunications. The purpose of NPSTC is to follow up on the recommendations of the Public Safety Wireless Advisory Committee (PSWAC). In addition, NPSTC acts as a resource and advocate for public safety telecommunications issues.



This snapshot was taken from an immersive visualization developed by ITL of the dynamics of concrete flow with embedded fibers. The data was obtained from a parallel simulation algorithm developed in collaboration with the NIST Building and Fire Research Laboratory.

Luke KleinBerndt and Nader Moayeri participate in Project Mesa: Broadband Mobile Communications for Public Safety.

NORTH AMERICAN OPEN MATH INITIATIVE (NAOMI)

Open Math is a standard for communicating mathematical objects between computer programs. Bruce Miller represents ITL in this organization and in the Open Math Society.

OBJECT MANAGEMENT GROUP (OMG)

OMG is a nonprofit international consortium of 500 organizations whose mission is to research, develop, and promote the use of object-oriented technology for distributed systems development. John Barkley is ITL's principal representative to OMG.

OPTICAL INTERNETWORKING FORUM (OIF)

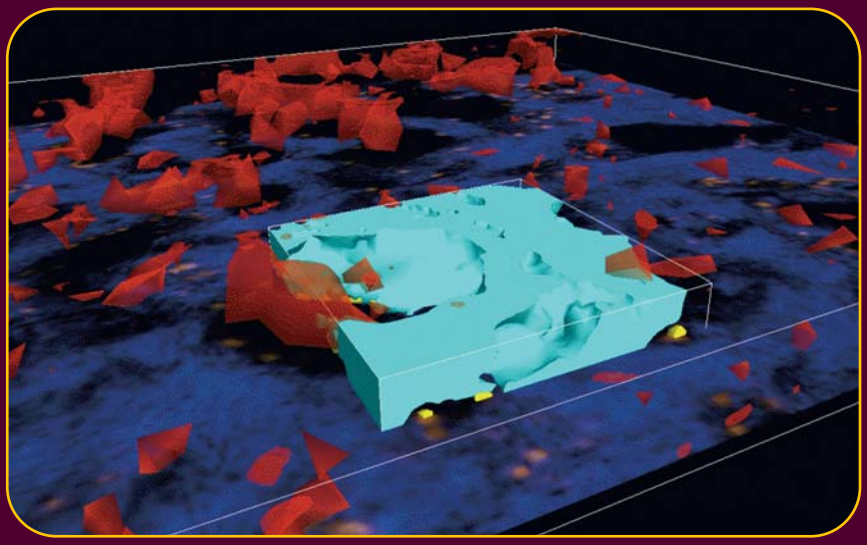
The OIF fosters the development and deployment of interoperable products and services for data switching and routing using optical networking technologies. David Su and David Griffith represent ITL in the Architecture, Internetworking, and Management groups.

OPTICAL STORAGE TECHNOLOGY ASSOCIATION (OSTA)

OSTA is an international trade association dedicated to promoting the use of writable optical technology for storing computer data and images. Xiao Tang, Fred Byers, and Oliver Slattery represent ITL.

ORGANIZATION FOR THE ADVANCEMENT OF STRUCTURED INFORMATION STANDARDS (OASIS)

OASIS is an international consortium dedicated to accelerating the adoption of product-independent formats based on public standards. These standards include XML and related XML-based recommendations as well as others that are related to structured information processing. Lynne Rosenthal, Michael Kass, and Mark Skall represent ITL. Our participation includes the development of conformance tests for these standards.



ITL is developing a variety of techniques to enable the immersive visualization of complex volumetric data. Here both high resolution (light blue) and low resolution (dark blue) scans of a polymer with growing cells (yellow and red, respectively) are combined in a single visualization.

SOCIETY FOR AUTOMOTIVE ENGINEERS (SAE)

SAE is a resource for technical information and expertise used in designing, building, maintaining, and operating self-propelled vehicles for use on land or sea, in air or space. Over 83,000 engineers, business executives, educators, and students from more than 97 countries share information and exchange ideas for advancing the engineering of mobility systems. Sandy Ressler participates in SAE-G13, Human Standards.

SOCIETY OF MOTION PICTURE AND TELEVISION ENGINEERS (SMPTE)

SMPTE is an international technical society devoted to advancing the theory and application of motion-imaging technology. Wo Chang serves on W25, Metadata Description.

TELECOMMUNICATIONS INDUSTRY ASSOCIATION (TIA) AND EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (ETSI)

The TIA is the leading U.S. nonprofit trade association serving the communications and information technology industry, with proven strengths in market development, trade shows, domestic and international advocacy, standards development and enabling e-business. The ETSI is an independent, nonprofit organization, whose mission is to produce telecommunications standards for today and for the future. Luke KleinBerndt and Nader Moayeri participate with these organizations on Project MESA: Broadband Mobile Communications for Public Safety.

WEB3D CONSORTIUM

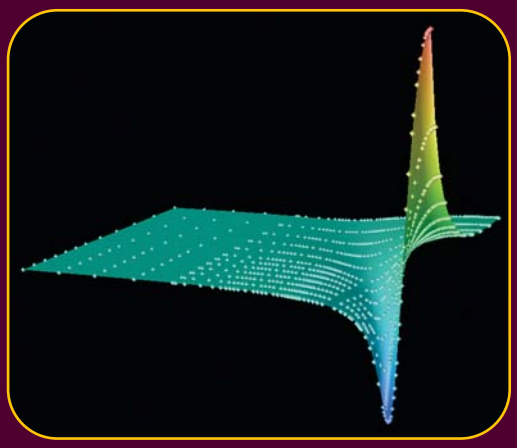
The Web3D Consortium provides a forum for the creation of open standards for Web3D specifications and accelerates the worldwide demand for products based on these standards through the sponsorship of market and user education programs. Sandy Ressler represents ITL on the MPEG Development Activity, the Humanoid Animation Working Group, and the Medical Working Group.

WORLD WIDE WEB CONSORTIUM (W3C)

The W3C is an international industry consortium created to lead the web to its full potential by developing common protocols that promote its evolution and ensure its interoperability. Mark Skall serves on the W3C Advisory Committee. Tim Boland represents ITL on the Authoring Tools Working Group (WG), the Authoring Tools Accessibility WG, and the Cascading Stylesheets WG. Bruce Miller serves on the Math Interest Group. Lynne Rosenthal, Mark Skall, and Sandra Martinez are involved in the Quality Assurance Activity. Carmelo Montanez-Rivera participates in the Query WG. Anthony Cincotta represents ITL on the Schema WG, Wo Chang on the SYMM WG, and Martinez on the XML WG. ITL's contributions facilitate web interoperability.

X9

X9 develops, establishes, publishes, maintains, and promotes standards for the financial services industry in order to facilitate delivery of financial products and services. Morris Dworkin participates in X9F, Data and Financial Information Security, and X9F.1, Cryptographic Tool Standards and Guidelines. Elaine Barker, Lawrence Bassham, Sharon Keller, and Annabelle Lee serve as Editors in X9F.1. Elaine Barker attends X9F.3, Cryptographic Protocols, and Annabelle Lee participates in X9F.5, Digital Signature and Certificate Policy. Through participation in this forum, ITL promotes the security of the financial services industry. ■



This visualization of the real part of a complex susceptibility function was obtained by ITL staff working with the NIST Electronics and Electrical Engineering Laboratory on models for transport in compound semiconductors.

PUBLICATIONS FY 2004

NIST SPECIAL PUBLICATIONS

SP 500-252	Care and Handling of CDs and DVDs-A Guide for Librarians and Archivists	October 2003
SP 500-255	The Twelfth Text Retrieval Conference	March 2004
SP 500-256	Improving the Usability and Accessibility of Voting Systems and Products	May 2004
SP 500-257	Proceedings of the ICASSP 2004 Meeting Recognition Workshop	September 2004
SP 500-258	Drive Compatibility Test (Phase 2) for DVD-R (General) and DVD+R Discs, Including DVD Creation Plan	September 2004
SP 800-27	Engineering Principles for IT Security (A Baseline for Achieving Security), Revision A	June 2004
SP 800-35	Guide to Information Technology Security Services, Recommendations of the National Institute of Standards and Technology	October 2003
SP 800-36	Guide to Selecting Information Technology Security Products, Recommendations of the National Institute of Standards and Technology	October 2003
SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems	May 2004
SP 800-38C	Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality	May 2004
SP 800-42	Guideline on Network Security Testing, Recommendations of the National Institute of Standards and Technology	October 2003
SP 800-50	Building an Information Technology Security Awareness and Training Program	October 2003
SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories	June 2004
SP 800-61	Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology	January 2004
SP 800-63	Electronic Authentication Guideline, Recommendations of the National Institute of Standards and Technology	June 2004
SP 800-64	Security Considerations in the Information System Development Life Cycle, Recommendations of the National Institute of Standards and Technology	October 2003
SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher	May 2004
SP 800-72	Guidelines on PDA Forensics, Recommendations of the National Institute of Standards and Technology	November 2004

FEDERAL INFORMATION PROCESSING STANDARDS		
FIPS 199	Categorization of Federal Information and Information Systems	February 2004
NIST INTERAGENCY REPORTS		
NISTIR 7034	2003 Information Technology Laboratory (ITL) Technical Accomplishments	January 2004
NISTIR 7043	Proceedings of the Biometric Consortium Conference 2003 (Volumes 1 and 2)	August 2004
NISTIR 7056	Card Technology Developments and Gap Analysis Interagency Report	March 2004
NISTIR 7059	1st Annual PKI Research Workshop Proceedings	October 2003
NISTIR 7067	Visualization and Data Mining in a 3D Immersive Environment: Summer Project 2003	October 2003
NISTIR 7083	Face Recognition Vendor Test 2002 Supplemental Report	February 2004
NISTIR 7085	2nd Annual PKI Research Workshop Proceedings	April 2004
NISTIR 7091	Towards a Framework for Evaluating Ubiquitous Computing Applications	March 2004
NISTIR 7100	PDA Forensic Tools: An Overview and Analysis	August 2004
NISTIR 7103A	Forensic Software Testing Support Tools: Test Plan, Test Design Specification, Test Case Specification	August 2004
NISTIR 7103B	Forensic Software Testing Support Tools: Test Summary Report	August 2004
NISTIR 7110	Matching Performance for the US-Visit IDENT System Using Flat Fingerprints	May 2004
NISTIR 7111	Computer Security Division 2003 Annual Report	April 2004
NISTIR 7112	Studies of Plain-to-Rolled Fingerprint Matching Using the NIST Algorithmic Test Bed (ATB)	April 2004
NISTIR 7119	Studies of One-to-One Fingerprint Matching with Vendor SDK Matchers	April 2004
NISTIR 7122	3rd Annual PKI R&D Workshop Proceedings	September 2004
NISTIR 7123	Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report	July 2004
NISTIR 7144	Integer Representation of Decimal Numbers for Exact Computations	October 2004
NISTIR 7150	Dublin Core and the Alternative Interface Access Protocol	August 2004
NISTIR 7151	Fingerprint Image Quality	August 2004
NISTIR 7162	Guide to Public Safety Applications of Wireless Technology	October 2004

ITL BULLETINS	
Information Technology Security Awareness, Training, Education, and Certification	October 2003
Network Security Testing	November 2003
Security Considerations in the Information System Development Life Cycle	December 2003
Computer Security Incidents: Assessing, Managing, and Controlling Risks	January 2004
Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems	March 2004
Selecting Information Technology Security Products	April 2004
Guide for the Security Certification And Accreditation of Federal Information Systems	May 2004
Information Technology Security Services: How to Select, Implement, and Manage	June 2004
Guide for Mapping Types of Information And Information Systems to Security Categories	July 2004
Electronic Authentication: Guidance for Selecting Secure Techniques	August 2004
Information Security Within the System Development Life Cycle	September 2004
Securing voice Over Internet Protocol (IP) Networks	October 2004
Understanding the New NIST Standards and Guidelines Required by FISMA	November 2004

CONFERENCES FY 2004

WORKSHOP ON CONTENT-BASED RETRIEVAL FROM DIGITAL VIDEO

On November 17-18, 2003, ITL and the National Security Agency's Advanced Research and Development Activity (ARDA) co-sponsored a workshop on content-based retrieval from digital video, which was attended by an international group of almost 50 researchers. The goal of the workshop was to advance content-based retrieval from digital video via open metrics-based evaluation. Twenty-four research groups, including ten groups from the U.S., ten from Europe, and four from Asia/Australia, participated in one or more of four tasks: shot boundary detection, story segmentation and typing, high-level feature extraction, and search. See *http://www-nlpir.nist.gov/projects/trecvid*.

TOPIC DETECTION AND TRACKING WORKSHOP ON TEXT ORGANIZATION

ITL hosted the annual Topic Detection and Tracking (TDT) Evaluation Workshop on November 17-18, 2003. The TDT program develops technologies that search, organize, and structure news-oriented textual materials from a variety of broadcast news media in the Arabic, English, and Mandarin languages. The research-driven program uses controlled laboratory simulations of hypothetical systems to test the efficacy of potential technologies to access the continuously flowing information that is available from news-producing entities. The website is *http://www.nist.gov/TDT*.

TEXT RETRIEVAL CONFERENCE (TREC)

ITL sponsored the twelfth Text REtrieval Conference (TREC 2003) held at NIST on November 18-21, 2003. TREC is a series of evaluation workshops designed to foster research on technologies for information retrieval. Participants produce retrieval results for one or more focus areas called tracks prior to the workshop, then meet during the workshop to discuss results. TREC 2003 contained six tracks, including tracks on question answering, retrieving web documents, and eliminating redundant information in a response. In addition to a new genomics track, two other new tracks focused on improving baseline retrieval effectiveness. The website is *http://trec.nist.gov*.

VOTING STANDARDS SYMPOSIUM

Over 280 computer scientists, vendors, voting rights activists, Secretaries of State, and local election officials participated in NIST's First Symposium on Building Trust and Confidence in Voting Systems in Gaithersburg on December 10-11, 2003. Participants discussed and debated challenging computer security and usability issues related to the Help America Vote Act (HAVA) and the role NIST would play in the law's implementation. The website is *http://vote.nist.gov*.

INFORMATION SECURITY WORKSHOP FOR SMALL BUSINESSES

As part of its outreach initiative, ITL sponsored an Information Security Workshop for Small Businesses in Orlando, Florida, at the Small Business Administration (SBA) Entrepreneur Center (NEC) on December 10, 2003. Attendees included Chief Information Officers and Comptrollers of small and medium-sized businesses and self-employed persons. The website is *http://csrc.nist.gov*.

HANDS-ON UNCERTAINTY IN MEASUREMENT WORKSHOP

Staff of ITL's Statistical Engineering Division gave a "Hands-On Workshop on Estimating and Reporting Measurement Uncertainty" to metrologists at the 2004 Measurement Science Conference in Anaheim, California. Attended by participants from industry and government, the workshop described the statistical framework and methods needed to develop uncertainty statements based on the *ISO Guide to the Expression of Uncertainty in Measurement*.

SYMPOSIUM ON KNOWLEDGE BASED AUTHENTICATION

ITL and the General Services Administration (GSA) co-sponsored a symposium on "Knowledge Based Authentication: Is it Quantifiable?" on February 9-10, 2004, at NIST. Approximately 150 people participated in the symposium. Knowledge Based Authentication (KBA) is a useful tool to remotely authenticate individuals who conduct business electronically with federal agencies or businesses infrequently. The symposium explored KBA through panel discussions of user requirements, KBA system models, and metrics to quantify information sources, questions for challenges, analysis and scoring of responses, and standards. Complete information can be found at *http://csrc.nist.gov/kba*.

WORKSHOP ON TECHNOLOGY TO ADDRESS SPAM E-MAIL

On February 17, 2004, ITL conducted a workshop on technology to address the growing problem of spam e-mail. About 130 people attended the workshop from the legislative and policy community; the enforcement community; Internet service providers (ISPs) and vendors; the community of those that must implement the technology; the research and academic community; and the normal, private end-users. The workshop brought experts from these various communities together for one of the first meetings of this type to be hosted by the federal government. The website is *http://csrc.nist.gov/spam/index.html*.

SECURITY CONTROLS WORKSHOP

ITL hosted a public workshop at NIST on March 8, 2004, to discuss the comments received, during the public comment period, on NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*. The workshop also addressed future plans for modifying and enhancing the security controls document. Over 250 attendees representing more than 100 organizations from the public and private sectors participated in the workshop. The website is *http://csrc.nist.gov/sec-cert/*.

FISSEA CONFERENCE

ITL and the Federal Information Systems Security Educators' Association (FISSEA), an ITL-supported, federally focused organization, co-sponsored its annual conference March 9-11, 2004, at the University of Maryland. FISSEA's focus is to elevate awareness and knowledge of information systems security throughout the federal government and to encourage the professional development of its members. The conference drew nearly 150 attendees, with presentations from more than 60 speakers that addressed information systems security awareness, training, education, and certification of information systems security professionals. The website is *http://csrc.nist.gov/fissea*.

INTERNATIONAL MEETING OF BIOMETRICS EXPERTS

ITL hosted the International Meeting of Biometrics Experts on March 23-25, 2004, in Gaithersburg. The purpose of the unique meeting was to support technical information sharing on biometrics between the various national biometrics testing laboratories as well as other appropriate organizations, in the hopes of leading to coordination of testing and evaluation procedures for the biometrics components of travel documents. The Department of Commerce, Department of Homeland Security, Department of State, Department of Justice, and the White House Office of Science and Technology Policy jointly organized the meeting. Presenters and attendees represented G-8 and other nations including Australia, Canada, European Commission, France, Germany, Hungary, Italy, Ireland, Japan, Korea, Malaysia, Mexico, Netherlands, Norway, Russia, Singapore, South Africa, Switzerland, the United Kingdom, and the United States.

PUBLIC KEY INFRASTRUCTURE (PKI) R&D WORKSHOP

On April 12-14, 2004, ITL hosted the 3rd Annual PKI R&D Workshop at NIST. Co-sponsors of the workshop included NIST, the National Institutes of Health, and Internet2 in cooperation with USENIX and OASIS. More than 120 security researchers attended the event. Workshop goals included cross-pollinating existing research efforts, identifying the key remaining challenges in deploying public key authentication and authorization, and developing a research agenda addressing those outstanding issues. The website is *http://csrc.nist.gov/pki/*.

11TH SPRING RESEARCH CONFERENCE ON STATISTICS IN INDUSTRY AND TECHNOLOGY

ITL hosted approximately 110 researchers from industry, government, and academia at the 11th Spring Research Conference on Statistics in Industry and Technology at

NIST from May 19-21, 2004. The Institute of Mathematical Statistics (IMS) and the Section on Physical and Engineering Sciences of the American Statistical Association (ASA/SPES) jointly sponsored the annual conference. The conference promotes cross-disciplinary research in statistical methods for engineering, science, and technology by bringing together statisticians, researchers in the application areas, and industrial practitioners working in these areas. The website is *http://www.itl.nist.gov/div898/conf/src2004/*.

RICH TRANSCRIPTION MEETING RECOGNITION WORKSHOP

ITL sponsored the Spring 2004 Rich Transcription Meeting Recognition Workshop at the annual IEEE International Conference on Acoustics, Speech, and Signal Process (ICASSP) on May 17, 2004, in Montreal, Canada. The event focused on technologies relevant to the automatic recognition and extraction of information from meetings. The meeting incorporated 23 technical papers/presentations in five areas: the 2004 Meeting Recognition Evaluation, data collection and transcription, speech processing research, related research, and related programs. The workshop brought together a burgeoning new community of researchers and government sponsors working in the meeting domain. The website is *http://www.itl.nist.gov/iaui/*.

WORKSHOP ON TRENDS IN MATHEMATICAL SOFTWARE

ITL hosted a workshop on the Changing Face of Mathematical Software on June 3-4, 2004, at George Washington University. The meeting provided a forum for commercial software vendors and academic and government researchers to discuss issues regarding the development, packaging, and dissemination of modern mathematical software libraries and systems. Twenty-six participants from six countries participated. The meeting was one of a yearly series of topical workshops sponsored by the International Federation for Information Processing's (IFIP) Working Group 2.5 (WG 2.5). Chartered by UNESCO in 1961, IFIP is a multinational federation of professional and technical organizations fostering international cooperation in the field of information processing. The website is at *http://math.nist.gov/workshops/wg25-2004/*.

CRYPTOGRAPHIC MODULE VALIDATION PROGRAM SYMPOSIUM 2004

On September 14-15, 2004, the Cryptographic Module Validation Program (CMVP), co-sponsored by NIST and the Communications Security Establishment (CSE) of Canada, held its third technical symposium. The event included presentations and discussions on Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, supporting documents such as the Derived Test Requirements and Implementation Guidance, cryptographic algorithm testing suites, expectations, future direction, panel discussions from federal and user agencies, and laboratory panel discussions. Over 110 participants from a broad base of the international community attended the conference. The website is *http://csrc.nist.gov/cryptval*.

BIOMETRIC CONSORTIUM CONFERENCE

On September 20-22, 2004, ITL co-sponsored the annual Biometric Consortium Conference in Crystal City, Virginia. One of the largest events worldwide dedicated solely to biometrics, the conference included a program with over 110 speakers presenting to more than 1,000 participants from over 50 government agencies, 25 universities, and 200 commercial technology vendors, systems integrators, and end users. The conference addressed the latest trends in biometrics research, development, testing and application of biometrics, and the important role that these technologies will play in the identification and verification of individuals in this age of heightened security and privacy. Government speakers highlighted the adoption of biometric standards in major government programs.

In addition to ITL, the National Security Agency (NSA), The National Biometric Security Project (NBSP), DoD's Biometrics Management Office (BMO), the National Institute of Justice (NIJ), West Virginia U.S.A., the General Services Administration (GSA), Office of Electronic Government and Technology, Office of Governmentwide Policy, and the National Science Foundation (NSF) co-sponsored the conference. Supporting organizations included the American National Standards Institute (ANSI), the BioAPI Consortium, the International Biometric Industry Association (IBIA), the InterNational Committee for Information Technology Standards (INCITS), and the Biometric Foundation. The website is *http://www.nist.gov/bc2004*. ■

STAFF RECOGNITION

DEPARTMENT OF COMMERCE 2004 MEDAL AND NIST AWARDS

The **NIST Smart Card Team**, consisting of (left to right) **John Wack**, **Teresa Schwarzhoff**, **James Dray**, all of the Computer Security Division, and **Alan Goldfine**, Software Diagnostics and Conformance Testing Division, received the 2004 Gold Medal Award for the development of a framework and specification that dramatically advanced interoperability among smart card applications, coalesced U.S. Government requirements, and forged alliances with the world's foremost authorities on smart cards. The work of the NIST Smart Card Team served to open an entire market to U.S. businesses while dramatically increasing the security of government agencies.

Mary Brady (from left), **Richard Rivello**, **Sandra Martinez**, **John Tebbutt**, and **Carmelo Montanez-Rivera**, Software Diagnostics and Conformance Testing Division, received a 2004 Bronze Medal Award for the development of conformance tests for the Extensible Markup Language (XML) standards. This work has had a momentous impact on facilitating interconnected systems as well as providing dramatic cost savings to companies developing and using these systems.

William Guthrie (second from left) and **Nien-Fan Zhang** (right), Statistical Engineering Division, received a 2004 Silver Medal Award, with colleagues Theodore Doiron (left) and Richard Silver (second from right) of NIST's Manufacturing Engineering Laboratory, for the development and calibration of a landmark two-dimensional grid Standard Reference Material (SRM 5001) through an innovative and effective collaboration with U.S. industry.

Mark Carson, Advanced Network Technologies Division, received a 2004 Bronze Medal Award for engineering achievement for developing the NIST Network Emulation Tool and pioneering the use of emulation as the basis for the test and evaluation of emerging Internet multimedia technologies. Carson's work changed the Internet industry's approach to the test and evaluation of performance sensitive applications.

Stefan Leigh, Statistical Engineering Division, received a 2004 Bronze Medal Award for exemplary leadership in expert application and dissemination of statistical metrology for the chemical, physical, and information sciences. Leigh was recognized for his broad impact on the quality of the NIST Standard Reference Materials (SRMs) through his contributions to uncertainty certification.

Timothy Burns, Mathematical and Computational Sciences Division, and seven NIST colleagues, members of the Kolsky Team, received the 2004 Allen V. Astin Award for advancements in measurement of dynamic material properties, leading to the first ever stress-strain measurements at high strain-rate and heating-rate. The advanced measurement capabilities developed by the team validate theoretical relations between microstructure transformation due to elevated temperatures and the resulting stress-strain behavior of the bulk material.

EXTERNAL RECOGNITION

Ivelisse Aviles, Statistical Engineering Division, received the Summer Research Opportunity Program (SROP) Alumni Achievement Award by the Committee on Institutional Cooperation. The award was presented at the SROP Conference held at the University of Iowa on July 10, 2004.

Wo Chang, Information Access Division, received the InterNational Committee for Information Technology Standards (INCITS) Technical Excellence Award for 2003. Chang was recognized for his invaluable contributions to the success of the INCITS L3.1 Moving Picture Experts Group (MPEG) program, which covers all MPEG standards including MPEG-1/-2/-4/-7/-21 and Advanced Video Codec as a joint project between the International Organization for Standardization and the International Telecommunications Union.

Alicia Clay, Deputy Chief, Computer Security Division, and **Michael Hogan**, Standards Liaison, Office of the ITL Director, received the first place award in the World Standards Day 2004 Paper Competition for their joint paper, "Securely Connecting the World with Cyber Security Standards." The paper was selected by the World Standards Day 2004 Planning Committee and the Standards Engineering Society, which published the article in the November/December 2004 issue of *Standards Engineering: The Journal of the Standards Engineering Society*.

Hamid Gharavi, Advanced Network Technologies Division, was elected by the Institute of Electrical and Electronics Engineers (IEEE) Communications Society as a Distinguished Lecturer on the topics of wireless multimedia communications and mobile ad hoc networks. Gharavi holds eight U.S. patents and has written a large number of publications related to these topics.

Joan Hash, Manager, Security Management and Guidance Group, Computer Security Division, received a 2004 Federal 100 Award from Federal Computer Week. Hash was recognized for providing principal direction to the development of security management guidelines and serving as key reviewer and often co-author to ensure overall quality and consistency with legal, policy, and other existing security guidelines.

Kevin Mills, senior research scientist in the Advanced Network Technologies Division, won the outstanding adjunct award for 2004, conferred by the Department of Information and Software Engineering (ISE) at George Mason University (GMU). Since receiving a Ph.D. in Information Technology from GMU in January 1996, Mills has served continuously on the ISE adjunct faculty.

Kotikalapudi Sriram, Advanced Network Technologies Division, is a co-recipient of one of the top five patented new technologies of 2003, as recognized by MIT's *Technology Review* magazine. Selected from thousands of patents issued by the U.S. Patent Office in 2003, the patent is on Quality of Service (QoS) Techniques for Voice Over Internet Protocol (VOIP). Sriram and colleagues developed the innovative technology while at Bell Laboratories in 1998.

Fernando Podio, Computer Security Division, was a co-recipient of the InterNational Committee for Information Technology Standards (INCITS) Gene Milligan Award for Effective Committee Management for 2003. The award recognizes individuals who, as officers, have provided outstanding leadership to the subgroup in its national and/or international work. Podio chairs the INCITS M1, Biometrics, Officers Team.

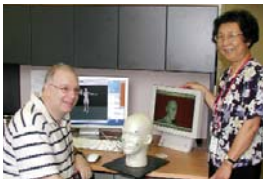
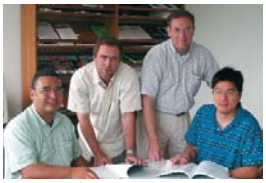
G.W. (Pete) Stewart, faculty appointee in the Mathematical and Computational Sciences Division, was elected to the National Academy of Engineering. Stewart is a Professor of Computer Science at the University of Maryland at College Park, as well as a Professor of the Institute for Advanced Computer Studies (UMIACS). Stewart was cited for development of numerical algorithms and software widely used in engineering computation.

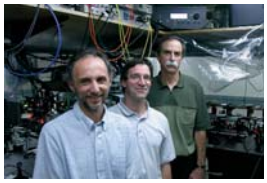
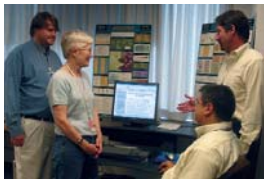
Thomas Ryan, guest researcher in the Statistical Engineering Division, was elected a Fellow of the American Society for Quality. Only about 40 of the 600 Fellows are statisticians.

Teresa Schwarzhoff, Computer Security Division, received an InterNational Committee for Information Technology Standards (INCITS) Service Award for 2003 for her contribution to the INCITS B10 committee on standardization of the U.S. Government Smart Card Interoperability Specification. Schwarzhoff's excellent work toward standardization of the specification had a clear and positive impact on national security and competitiveness of the U.S. smart card industry.

THE PEOPLE OF ITL

TONAN AGBOTA JEROME AJOT NEGA ALEMAYEHU DANIEL ALLEN BRADLEY ALPERT ENRIQUE AMIGO CABRERA PAUL AMMANN DANIEL ANDERSON EMMANOUIL ANTONAKAKIS BRIAN ANTONISHEK MICHAEL ARCHER JOAQUIM ARLANDIS NAVARRO WILLIAM ASHLEY JOHN ATKINS JULIEN AUBE WHITNEY AUSTIN ANA AVILES RICHARD AYERS DOUGLAS BACCI ERIC BAER RICHARD BAILEY STEPHANY BAILEY LAUREN BALLOU KOICHIRO BAN BARRY BANNISTER BRUCE BARGMEYER ELAINE BARKER WILLIAM BARKER JOHN BARKLEY JR LAWRENCE BASSHAM III ISABEL BEICHL JACKIE BELL GEORGE BENNETT JAVIER BERNAL BARRY BERNSTEIN ROBIN BICKEL RAMSEY BILLUPS PAUL BLACK DEBORA BLACKSTONE CHAD BLOMQUIST DUANE BOES ROBERT BOHN RONALD BOISVERT FREDERICK BOLAND JR JANET BOODRO OLIVER BORCHERT PAULINE BOWEN MARY BRADY DENNIS BRANSTAD RICHARD BRAUN FLORENT BREGAND TANYA BREWER-JONEAS RONNIE BRITTON CHRISTOPHER BROWN THOMAS BUCKINGHAM LORI BUCKLAND LORNA BUHSE STEPHEN BULLOCK SHAUNTIA BURLEY TIMOTHY BURNS WILLIAM BURR FREDERICK BYERS ZHONGPING CAI DOMENIC CAPPABIANCA ALFRED CARASSO LISA CARNAHAN ROBERT CARPENTER MARK CARSON SARA CASWELL JOHN HODOL CHAI RAMASWAMY CHANDRAMOULI JOSHUA CHANG RICHARD CHANG SHU-JEN CHANG WO CHANG ABDERAHMAN CHENIOUR MICHAEL CHERNICK NICOLAS CHEVROLLIER JAE CHUNG NICOLAS CILLEROS ANTHONY CINCOTTA ALICIA CLAY KEVIN COAKLEY KENDRA COLE LESLIE COLLICA JOYCE CONLON JOHN COOK DAVID COOPER CHRISTOPHER COPELAND JOHN CORNELL DAVID COTRELL CEDRIC COULON CARROLL CROARKIN MICHAEL CROWSEY TRUDY CUMMINGS RICHARD CURTIN DAVID CYPHER CHRISTOPHER DABROWSKI ERIC DALCI HOA DANG RONAN DANIELLOU PAMELA DAVIS JEAN DERUELLE JUDITH DEVANEY DIPAK DEY GIUSEPPE DI LORENZO ANDREW DIENSTFREY ALDEN DIMA DARRIN DIMMICK GEORGE DODDINGTON DONNA DODSON KIRK DOHNE MICHAEL DONAHUE JAMES DRAY JR MORRIS DWORKIN RANDALL EASTER CYNTRICA EATON LOWELL ELFENBEIN ALLAN EUSTIS BRUCE FABIJONAS EDWARD FANNING MATTHEW FANTO BRENDAN FARRAR-FOLEY CHARLES FENIMORE DAVID FERRAIOLO HILDEGARD FERRAIOLO JAMES FILLIBEN ANTOINE FILLINGER JONATHAN FISCUS LARRY FITZWATER PATRICIA FLANAGAN MARY FLOYD ELIZABETH FONG JEFFREY FONG JOHN FOUNTAIN KIMBERLY FOX SHEILA FRANKEL ELAINE FRYE LEONARD GALLAGHER KATHLEEN GALLO ROBERT GALLUP JINGSI GAO SHAOSHUAI GAO JOHN GAROFOLO MICHAEL GARRIS SAUL GASS SERBAN GAVRILA LEONARD GEBASE CAMILLO GENTILE WILLIAM GEORGE HAMID GHARAVI SUBHRA GHOSH ANDREW GIBBS MELISSA GIBSON DAVID GILSINN DONALD GISH SCOTT GLANCY AFZAL GODIL SYLVIA GOLDEN ALAN GOLDFINE NADA GOLMIE LAURA GOODING TIMOTHY GRANCE MARTHA GRAY KATHERINE GREEN TERENCE GRIFFIN DAVID GRIFFITH JR PATRICK GROTHER KATHARINE GURSKI WILLIAM GUTHRIE BARBARA GUTTMAN JON GWINN SEUNG-ILL HAAN JOHN HAGEDORN ROBERT HAGWOOD JAN HANNIG JOELLEN HANSROTH DONNA HARMAN GERLINDE HARR EDWARD HARRIS VICKIE HARRIS JOAN HASH NELSON HASTINGS KRISTI HAWES NATHANIEL HECKERT SYDNEY HENRARD JOSEPH HENRIQUEZ MARTIN HERMAN BARRY HERSHMAN THOMAS HEUTE RICKY HILDERBRAND PEGGY HIMES ROBERT HITCHO MICHAEL HOGAN DIANE HONEYCUTT THOMAS HOPPER ADRIANA HORNIKOVA PAMELA HOUGHTALING YING-PO HSIAO CHUNG TONG HU I-FENG HUANG MICHEAL HUBER JENNIFER HUCKETT WILLIAM HUFF ELIZABETH HUGHES RICHARD HUGHES HOWARD HUNG FERN HUNT MICHAEL INDOVINA KATRINA INGRAM MICHAELA IORGA HARIHARAN IYER FIROUZEH JALILIAN STANLEY JANET JR WAYNE JANSEN JAMES JASINSKI DYAMI JENKINS VON AYRE JENNINGS OLAF JERDE JANET JING ARNOLD JOHNSON SOREN JOHNSON RAGHU KACKER KAREN KAFADAR ATHANASIOS KARYGIANNIS DOMINIK KASPAR MICHAEL KASS STUART KATZKE ANTHONY KEARSLEY SHARON KELLER JOHN KELSEY JOHN KELSO EDWARD KENNEDY HOWARD KERMISCH CHRISTOPHE KERN PETER KETCHAM LAWRENCE KEYS CHOON SOO KIM CHUL KIM ELAINE KIM OKHEE KIM SEUNG HYUN KIM KELLY KIPFERL RICHARD KISSEL LUKE KLEIN-BERNDT ARTHUR KLEPCHUKOV KENTON KLINE STEPHAN KLINK EMANUEL KNILL JOSEPH KONCZAL HSIAO-MING KOO VLADIMIR KOROLEV RAMAKRISHNAN KRISHNAN DAVID KUHN SRIKANTA KUMAR JOHN LEE KUNTZ BYUNG-JAE KWAK MARY LAAMANEN STEPHEN LANGER CHRISTOPHE LAPRUN LYNNE LARKIN MARIANNE LARKIN JONATHAN LASKO SHARON LASKOWSKI JOHN LATTA DEBRA LAUTERBACH JAMES LAWRENCE MICHAEL LE TONY LE NANCY LEATHERMAN DENNIS LEBER YANN LEBLEVEC ANNABELLE LEE CALEB LEE

SUKYOUNG LEE JULIEN LEFORT STEFAN LEIGH NEGA LEMAYEHU ELIZABETH LENNON WALTER LIGGETT JR HUNG-KUNG LIU BENJAMIN LIVELSBERGER SUSAN LOAR SAMUEL LOMONACO BENJAMIN LONG TERRANCE LOSONSKY DANIEL LOZIER JOHN LU RICHANG LU CHRISTOPHE LUCAS JAMES LYLE GORDON LYON LIJUN MA KATHERINE MACFARLAND WILLIAM MAJURSKI DONALD MALEC JOCELYN MALONES VLADIMIR MARBUKH KAREN MARSHALL ALVIN MARTIN EDUARDO MARTINEZ VECINO SANDRA MARTINEZ PAUL MATTHEWS LEONARD MAXIMON ROBERT MCCABE ANDREW MCCAFFREY MARJORIE MCCLAIN JANET MCCULLOCH-BASS GEOFFREY MCFADDEN STEVEN MEAD KATHRYN MEADOW ORLANS KETAN MEHTA ROSS MICHEALS MARTIAL MICHEL BRUCE MILLER LEONARD MILLER KEVIN MILLS ALAN MINK WILLIAM MITCHELL NADER MOAYERI FRANCESCO MOGGIA VAN MOLINO CARMELO MONTANEZ-RIVERA DOUGLAS MONTGOMERY STANLEY MOREHOUSE KIMBERLY MORGAN ROY MORGAN EMILE MORSE LEE MOSER YOUSSEF MSELLEK CAROLYN MULFORD BRUCE MURRAY ANASTASE NAKASSIS BERTRAND NDZANA JUSTIN NEAL JAMES NECHVATAL PATRICIA NELSON HAN NGO ANNA NHAN ALEXEI NIKOLAEV FERNANDO O'CONNOR EARLE O'DONNELL JEFF OFFUTT AGNES O'GALLAGHER MICHAEL OGATA DIANNE O'LEARY FRANK OLVER PATRICK O'REILLY II PATIMA OUASRI PAUL OVER DAVID PALLETT DANNY PAN SANGWOO PARK YOLANDA PARKER HERBERT PATTERSON HARRIET PECK JAN-WEN PENG JOANNE PERRIENS ADELE PESKIN JULIA PETROUSKY JONATHON PHILLIPS SHASHI PHOHA FERNANDO PODIO MARGARET POLINKOVSKY WILLIAM POLK BERT PORTER DONALD PORTER FRANCES PORTER IRIS PORTNY FLORIAN POTRA ROLDAN POZO NICOLAS PRATZ MARK PRZYBOCKI GEORGE QUINN STEPHEN QUIROLGICO SHIRLEY RADACK NICOLAS RADDE MUDUMBAI RANGANATHAN OLIVIER REBALA LARRY REEKER MICHAEL REILLY ERIC RENAULT SANFORD RESSLER THOMAS RHODES MEGAN RICHTER ANN RICKERDS KELSEY RIDER CLEMENT RIDORET RICHARD RIVELLO EDWARD ROBACK JOHN ROBERTS KAMIE ROBERTS CEDRICK ROCHET ALLEN ROGINSKY MARK ROSE SCOTT ROSE JOAN ROSENBLATT LYNNE ROSENTHAL RONALD ROSS PERRINE ROUCOUX RICHARD ROUIL JULIE ROUZAUD EUGENE ROWE MYRON RUBINFELD ANDREW RUKHIN CRAIG RUSSELL BERT RUST THOMAS RYAN VITO SABIA HASSAN SAHIBZADA HASSAN SAHIBZAZA LUCY SALAH DENISE SANDERS GREGORY SANDERS DARRIN SANTAY KAROLINA SARNOWSKA STEVEN SATTERFIELD GEORGE SAUER BONITA SAUNDERS KAMRAN SAYRAFIAN-POUR ROBERT SCHMIECH JEAN SCHOLTZ CATHY SCHOTT TERESA SCHWARZHOFF ROBERT SCOTT MEGAN SEAMAN NELL SEDRANSK PHILIPPE SENELAS CLEMENT SEVEILLAC CHARLES SHEPPARD DA SHI MYUNG KI SHIN SANG-HEON SHIN KELLY SHUGGARS JAMES SIMS MARK SKALL OLIVER SLATTERY ROBERT SNELICK STANLEY SNOUFFER JR DOROTHY SNYDER IAN SOBOROFF WON-KYU SOHN YEUNG JOON SOHN DAVID SONG NAH-OAK SONG HAROLD SORRELL JUAN SOTO JR MURUGIAH SOUPPAYA MICHAEL SOURYAL TERESA SPLAIN JOLENE SPLETT SIVA SRINIVASAN KOTIKALAPUDI SRIRAM VINCENT STANFORD GILBERT STEWART WILLIAM STILLWELL GAROLD STONE WILLIAM STRAWDERMAN SARAH STREETT DAVID SU VERNA SUIT FRANCIS SULLIVAN SUZANNE SULLIVAN VASUGHI SUNDRAMOORTHY MARIANNE SWANSON ELHAM TABASSI CERYEN TAN HAI TANG XIAO TANG JOHN TEBBUTT ANDREW TESCHER MARY THEOFANOS BLAZA TOMAN AUDREY TONG PHUONG TON-NU PATRICIA TOTH SAMUEL TRAHAN SHARON TRAVIS DAVID TURNER DOMINIC VECCHIA ANGEL VILLALAIN PETER VLASOV JOHN WACK CHIH-MING WANG QIMING WANG KELLY WATKINS CRAIG WATSON CHARLES WAYNE SHARON WENTLING BARBARA WHEATLEY DOUGLAS WHITE JEANNETTE WILLIAMS CHARLES WILSON MARK WILSON CLARE WITTE CHRISTOPH WITZGALL BRIAN WLADKOWSKI STEPHEN WOOD JIN WU JOAN WYRWA BO YAN GRACE YANG MINGHUI YANG JAMES YEN JOONSOHN YEUNG ANOCHA YIMSIRIWATTANA JEFFREY YOUNG MICHELLE YOUNG ABDOU YOUSSEF MIKE YU JIAN YUAN JULIE ZANON SUSAN ZEVIN JIA ZHANG NIEN-FAN ZHANG JIAN ZHENG

Writer/Editor:
Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology

Design/Production:
Michael James, The DesignPond


STATIC RAM