INFORMATION TECHNOLOGY LABORATORY

Technical Accomplishments

2001

Enabling a Better Future

NISTIR 6815

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

CONTENTS

NISTIR 6815
NOVEMBER 2001

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond
Under Secretary for Technology

National Institute of
Standards and Technology
Arden L. Bement, Jr., Director

DIRECTOR'S FOREWORD

Welcome to the Information Technology Laboratory (ITL). As one of the National Institute of Standards and Technology (NIST) Laboratories, our mission is to develop and promote measurement, standards, and technology for information technology (IT) to enhance productivity, facilitate trade, and improve the quality of life. We also develop computer security standards and guidelines for the federal government in fulfillment of a legislative mandate. Working in partnership with industry, academia, government, and consortia, we develop and demonstrate tests, test methods, reference data, proof-of-concept implementations, and other IT infrastructure technologies. Our goal is to enable the future of the U.S. IT industry to produce products and services that are high quality, reliable, interoperable, and secure.

ITL made significant strides forward this year in critical research and standards areas. Industry, government, academia, and consortia recognized the valuable contributions of our work, including:

ANSI/NIST Image Standard for the Interchange of Fingerprint, Facial and Scar Mark, and Tattoo Information – ITL was instrumental in the development of this image data exchange standard, enabling crucial new applications in law enforcement;

Security/Critical Infrastructure Protection (CIP) – ITL administered the CIP grants program, providing $5 million in funding for nine research grants that will enhance security for critical infrastructures such as electrical grids and air traffic control systems;

William O. Mehuron, ITL Director

Advanced Encryption Standard (AES) – ITL's AES development team received the RSA Public Policy Award. Published as Federal Information Processing Standard (FIPS) 197, the AES will be the standard way to encrypt government content in the future. The AES will replace the Data Encryption Standards (DES); see *http://www.nist.gov/director/prog-ofc/report01-2.pdf* for an analysis of the economic impact of DES;

E-Book/Braille Reader – The ITL development team received the prestigious 2001 R&D 100 Award for the development of technology that could enhance accessibility to the Internet and electronic media for the visually impaired;

Extensible Markup Language (XML) – ITL released the XML Test Suite, Second Edition (+2000 tests), which is considered the metric for testing XML processors. We are also developing a reference implementation for the registry/repository of XML vocabularies for use in vertical markets;

Digital and Interactive TV – ITL developed the NIST Digital TV Application Software Environment (DASE) Reference Implementation, which provides application developers and consumer electronic manufacturers an application development environment and a basis for an interoperable digital TV receiver implementation. This is a major accomplishment for the digital TV industry, as all analog transmission is mandated by the FCC to be digital in 2007;

JavaNumerics - ITL chairs the Java™ Grande Forum's Numerics Working Group, which works with Sun Microsystems to implement changes in Java's specifications that admit much faster execution (up to ten times faster) for computing-intensive applications;

Wireless Personal Area Networks - ITL is addressing important technical issues, such as the critical issue of wireless palmtop computers crowding the unregulated 2.4 GHz-frequency band for small wireless pico-cellular networks; and

Scientific Applications and Visualization - ITL's work enabled NIST physicists to discover unknown properties of super-cooled matter, known as Bose-Einstein condensates, through unique computation and visualization techniques. NIST Senior Scientist Eric Cornell is a co-recipient of the 2001 Nobel Prize for Physics for pioneering work in this breakthrough area.

We continued our laboratory-wide pervasive computing initiative, focusing on smart space integration, pervasive software tools, and pervasive networking technology. We are working with industry partners in vital areas of human computer interaction, such as speech and visual recognition and tracking, sophisticated information access from multimedia databases, extensive information presentation capabilities, collaborative working environments, dynamic networking, security, and reliability. To ensure access for people with disabilities, ITL sponsored a major IT Accessibility Conference this year. Our collaboration with NIST's Physics Laboratory on quantum computing and quantum information systems moved forward, as did our work in biometrics and smart cards.

We continued to provide research collaborations and technical services to the NIST laboratories. The Mathematical and Computational Sciences Division and the Statistical Engineering Division support work in other NIST laboratories and perform crucial services such as modeling and certification of Standard Reference Materials (SRMs). Further, ITL provides vital services to the entire NIST community, including networking, high performance computing, support for desktop computers and workstation machines, the telephone system, and a host of other infrastructure activities. ITL also hosts the office of the NIST Chief Information Officer.

We appreciate your interest in the Information Technology Laboratory. In partnership with industry, government, and academia, we will continue to enable the future of the Nation's measurement and standards infrastructure for information technology.

William O. Mehuron, Director
Information Technology Laboratory
Web: http://www.itl.nist.gov
E-mail: itlab@nist.gov

ITL AT A GLANCE

William O. Mehuron, *ITL Director and Acting NIST Chief Information Officer (CIO)*

Susan F. Zevin, *Deputy Director*

Bruce Rosen, *Office of the CIO*

Catherine Nicoletti, *Acting Assistant Director for Boulder*

Kamie Roberts, *Associate Director for Federal and Industrial Relations*

Robert Glenn, *IT Security Office*

Kendra Cole, *Senior Management Advisor*

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

David Su, *Acting Chief of Advanced Network Technologies Division*

Edward Roback, *Chief of Computer Security Division*

Martin Herman, *Chief of Information Access Division*

Victor McCrary, *Chief of Convergent Information Systems Division*

Raymond Hoffmann, *Chief of Information Services and Computing Division*

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

Nell Sedransk, *Chief of Statistical Engineering Division*

Susan F. Zevin,

ITL Deputy Director

ITL MISSION

Our goals are to develop and promote measurement, standards, and technology for information technology (IT) to enhance productivity, facilitate trade, and improve the quality of life and to provide NIST with high-quality information technology services.

ITL CUSTOMERS

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

ITL PRODUCTS AND SERVICES

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

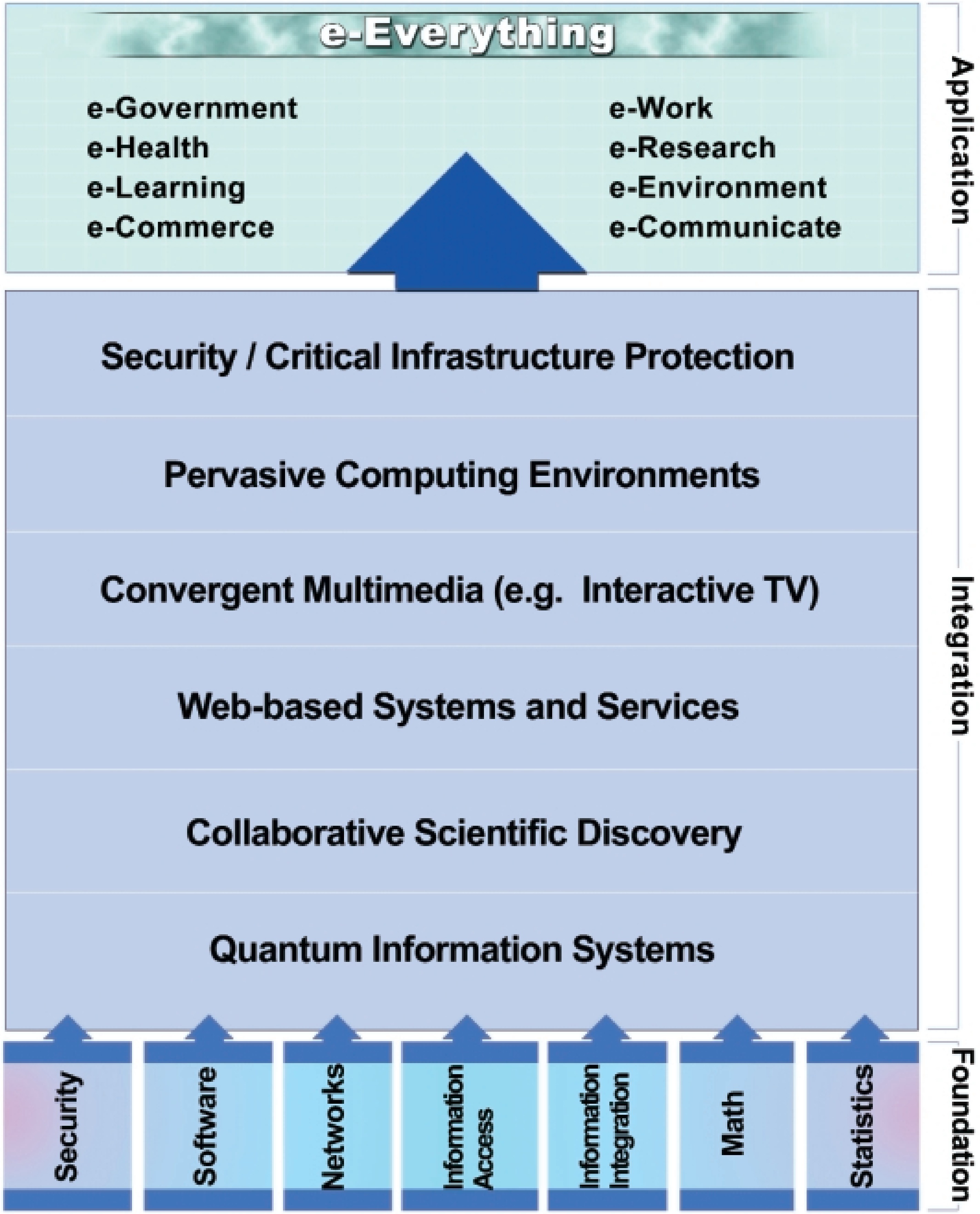
ITL RESOURCES

- highly qualified professional and support staff of 487 (includes part-time and faculty appointments), supplemented by 126 guest researchers (as of September 22, 2001)
- total authorization for fiscal year 2001 budget of $95.0M, all sources
- research facilities in Gaithersburg, Maryland, and Boulder, Colorado
- opportunities for cooperative research and interaction with industry and academia

ITL RESEARCH PROGRAM

The following chart represents the ITL Research Blueprint, the framework by which we describe our research program. Our seven research divisions provide a crucial foundation in information technology measurements and standards and these efforts are integrated into cross cutting areas such as critical infrastructure protection and pervasive computing. This thorough research approach provides enabling technologies necessary to achieve the promise of all e-Applications.

ITL RESEARCH BLUEPRINT



Application

e-Everything

e-Government
e-Health
e-Learning
e-Commerce

e-Work
e-Research
e-Environment
e-Communicate

Integration

Security / Critical Infrastructure Protection

Pervasive Computing Environments

Convergent Multimedia (e.g. Interactive TV)

Web-based Systems and Services

Collaborative Scientific Discovery

Quantum Information Systems

Foundation

Security

Software

Networks

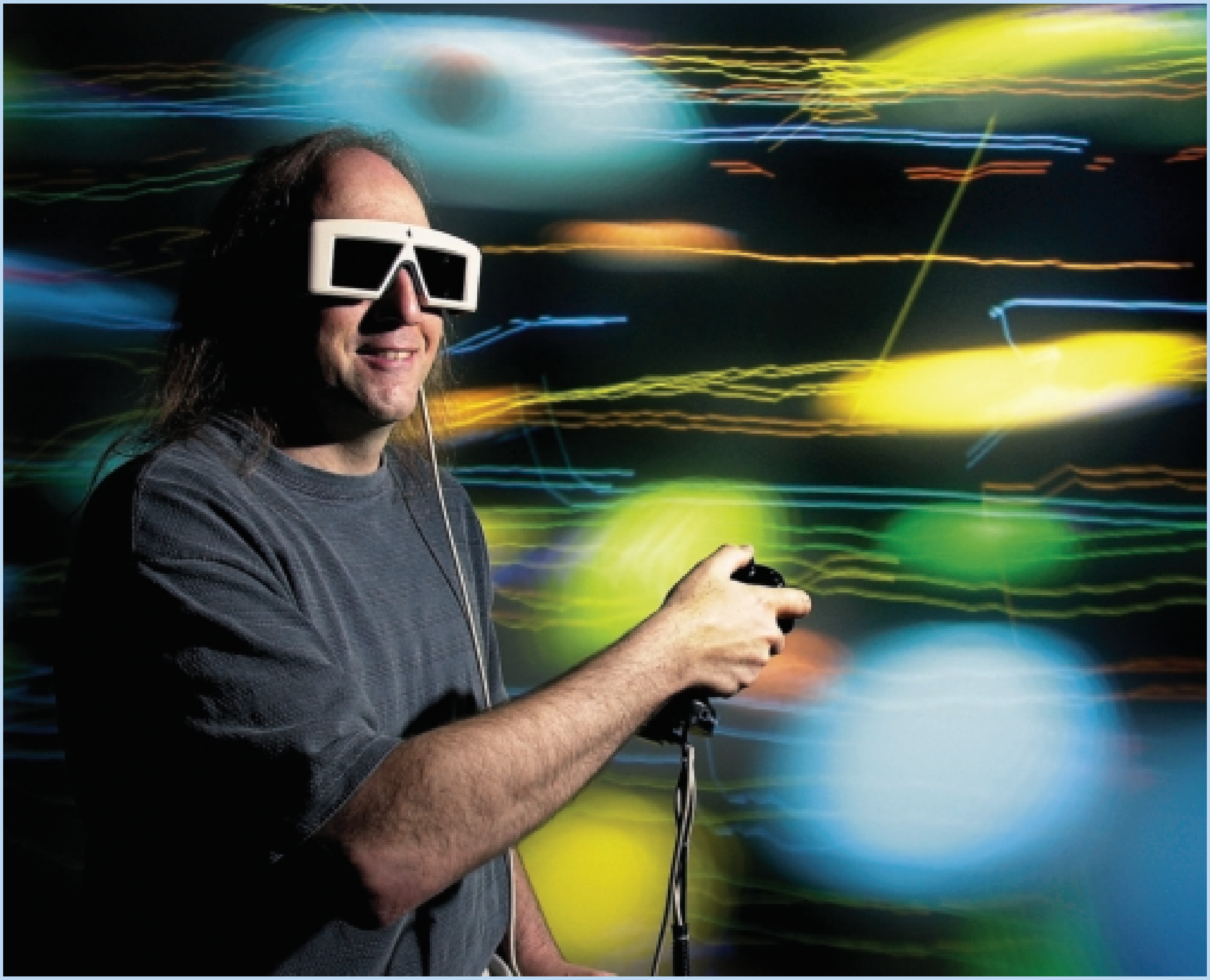
Information Access

Information Integration

Math

Statistics

ACCOMPLISHMENTS
OF OUR RESEARCH PROGRAM



Steven Satterfield studies a 3-D visualization of idealized particles inside wet concrete using a RAVE device. Reprinted with permission of Government Computer News, Copyright© Post Newsweek Tech Media Group.

SECURITY

BIOMETRICS AND SMART CARDS

ITL is assisting industry and government in the deployment and use of biometrics and smart card technologies. Working with the Biometric Application Programming Interface Consortium (BioAPI), ITL spearheaded the development of the Common Biometric Exchange File Format (CBEFF), a biometric data format that greatly facilitates the integration of biometric technologies into networks that have important mass commercial applications. We are also leading the development of the Government Smart Card (GSC) interoperability specification. Additionally, we are developing conformance tests and a testing program for the GSC specification. In FY2001, we developed a high-level technology roadmap for the GSC effort, established the GSC Interagency Advisory Board, completed the test plan for Phase I (Card Edge Interface), tested file system smart cards using the plan, and provided technical refinements on the GSC interoperability specification. We also contributed to the smart card protection profile and corresponding evaluation methodology.

For the law enforcement community, we are advancing standards and evaluation technology for interoperable Criminal Justice Information Systems (CJIS), providing standard reference implementations of fingerprint-related software. For the Department of Defense, we are developing evaluation methods and test data for biometric systems that operate at long distances from the subject (HumanID). In FY2001, we obtained American National Standards Institute (ANSI) approval for the final version of the Data Format for the Interchange of Fingerprint, Facial, and Scar Mark & Tattoo (SMT) Information (ANSI/NIST-ITL 1-2000), providing crucial interoperability in support of the CJIS. We published the NIST Fingerprint Image Software CD-ROM, which was needed as an interface to fingerprint Standard Reference Data. For the HumanID project, we designed and implemented data collection protocols and released metadata and face databases to customers and research collaborators. We implemented scoring software to measure HumanID recognition performance and defined new methods for analyzing, evaluating, and comparing recognition algorithms. The website is *http://www.itl.nist.gov/div895/isis/projects/biometricsproject.html*.

CRYPTOGRAPHIC STANDARDS AND APPLICATIONS

ITL is providing a toolkit of secure cryptographic algorithm standards, standardized security protocols and techniques, with tests for correct implementations, interoperability and assurance. In FY2001, the Secretary of Commerce announced NIST’s selection of the Rijndael algorithm to be proposed as the Advanced Encryption Standard (AES) in a Federal Information Processing Standard (FIPS). The Secretary announced approval of FIPS 197 in December 2001. Other cryptographic FIPS are being updated to provide commensurate levels of security.

Pauline Bowen and Kathy Lyons-Burke plan the activities of ITL's Computer Security Expert Assist Team.

Vickie Harris, Katie Shuggars, and Kelly Watkins learn details of the new Travel Manager system in ITL's Computer Security Division to support its travelers.

We conducted two workshops for modes of operation for symmetric key block ciphers and are planning one in FY2002 to develop a public key-based key management standard. To enable the deployment of cryptography, we collaborated with the Federal Deposit Insurance Corporation and the General Services Administration to develop a high-level Application Programming Interface (API) for public key-based cryptographic services. This API allows PKI-enabled applications to use PKI clients from any vendor. We also completed the Certificate Issuing and Management Components protection profile and a Directory Profile for the Federal PKI to address naming and other interoperability issues. We supported the Federal PKI Steering Committee and subcommittees, including the development of the Federal Bridge Certification Authority (FBCA), which became operational in June 2001.

More efficient, secure, and interoperable information systems and electronic commerce will be enabled through the NIST toolkit of standard algorithms, protocols, and techniques. It will be easier to build secure, interoperable applications with high-assurance products that implement needed cryptographic security functionality. The website is *http://csrc.nist.gov/encryption/*.

SECURITY MANAGEMENT AND GUIDANCE

For many years, ITL has had statutory responsibilities for developing information technology security standards and guidelines for protecting sensitive unclassified information in federal IT systems and networks. We develop computer security policy and management guidance for federal agencies, and we provide tools, techniques, and databases to protect against economic loss or injury due to disruption of critical federal systems and/or services. Those in the private sector use many of our products on a voluntary basis.

In FY2001, we published seven guidance documents on the following topics: PKI, random number generation, IT security engineering principles, security assessment framework, self-assessment, intrusion detection, and mobile code/active content. Drafts are in process on six additional topics. We also published five ITL Bulletins with a security focus.

We established the Computer Security Expert Assist Team (CSEAT), developed the CSEAT methodology, initiated the CSEAT program to provide automated information security program reviews of federal agencies, and completed the first CSEAT review. This review, completed for the Federal Emergency Management Agency, was well received. The website is *http://cseat.nist.gov*.

We defined a plan for conducting small- and medium-sized business regional security meetings and for developing appropriate educational material.

As a result of our security management and guidance program, agencies can more easily and cost-effectively address their computer security policy and management needs, issues, and problems. Agencies can use standard, tested solutions (such as best practices), avoiding duplication of effort and resources. Our Computer Security Resource Center is one of the most visited websites at NIST: *http://csrc.nist.gov*.

SECURITY OF EMERGING TECHNOLOGIES

ITL is identifying emerging information technologies impacting critical infrastructures, defining standards during the initial stages of these technologies and focusing on their security implications. By early participation in the development of standards, tests, test methodologies, assurance metrics, and reference materials for emerging technologies, we gain hands-on experience and insights into new technologies. We then can produce timely technical guidance for agencies and others in the secure use of these new technologies.

Focus areas include intrusion detection, role based access control (RBAC), authorization management, automated security testing, mobile agents, Internet Protocol security (IPsec), the ICAT metabase (a web-based index of 2,700 vulnerabilities with over 75,000 hits per month), critical infrastructure protection (CIP) grants (nine issued in FY2001), and technical guidance. We completed the second draft of the RBAC standard, which received acceptance by the National Committee for Information Technology Standards as a fast-track standard. Sun cites NIST's RBAC work in their flagship Solaris implementation. We enhanced and released PlutoPlus 2.0; NAI Labs adopted PlutoPlus as the basis for an SNMP-based IPsec Policy Management product. We demonstrated several privilege management components for mobile agents and completed a working mobile agent prototype demonstration. The website is *http://csrc.nist.gov/focus_areas.html#research*

SECURITY TESTING

Our security testing program includes cryptographic security testing, the Cryptographic Module Validation Program (CMVP), the National Information Assurance Partnership (NIAP), the Common Criteria (CC) Evaluation and Validation Program, International Recognition Arrangements, testing laboratory accreditation, automated security testing and test suite development, industry forums, and education, training, and outreach programs. In FY2001, the Secretary of Commerce approved the updated FIPS 140-2, Security Requirements for Cryptographic Modules. More than 170 products have received certificates of validation to date and a fifth testing laboratory was accredited this year.

The CC Recognition Arrangement was expanded to 14 nations, adding Israel. Under the auspices of NIAP, a joint NIST-National Security Agency program, we co-sponsored a government/industry IT security forum to identify strategies for the development of IT security requirements and specifications for the protection of government, business, and personal computing and real-time control systems. We participated in the second International CC Conference, as well as in a number of NIAP and CC workshops. We worked with the insurance industry to initiate an industry requirements forum. In the area of healthcare, we contributed to protection profiles for security and electronic signature standards for healthcare, as well as patient admission, discharge, and transfer system applications. We assisted Japan in building a CC testing program. We taught multiple protection profile classes. Through NIAP and the CMVP, we provided assistance to a number of federal and state agencies, industry corporations, research laboratories, and professional and trade associations.

The impact of our IT security testing programs is significant. Our programs provide timely, cost-effective IT security testing, increased security in IT systems through the availability of tested products, and the creation of business opportunities for vendors of security products, testing laboratories, and security consultants. The websites are *http://www.nist.gov/cmvp and http://niap.nist.gov.*

Peter Mell discusses the intrusion detection testing software with students Michael Reilly and Derek Dye.

ACCOMPLISHMENTS OF OUR RESEARCH PROGRAM

SOFTWARE

Martha Gray and Jim Lyle analyze computer forensics test procedures to make sure test results will be rigorous and meet the high quality needs of the law enforcement community.

COMPUTER FORENSICS

Computer forensics is rapidly becoming recognized by the legal and law enforcement communities as a science on a par with the other forensic sciences. As this trend continues, it will become even more important to handle and examine computer evidence properly. The National Institute of Justice, the Federal Bureau of Investigation, and the Department of Defense Computer Forensics Laboratory asked ITL to provide a neutral and technically proficient source of reference data and test procedures.

In FY2001, we developed the National Software Reference Library (NSRL), a repository of known software, file profiles, and file signatures. More than 1000+ products and 1,000,000 file profiles populate the library. The Computer Forensics Tools Testing project provides a measure of assurance that the tools used in the investigations of computer-related crimes produce valid results. We continued to develop tests and procedures for forensic tools, including the Disk Imaging Requirements Specification and tests for disk imaging tools. We contacted law enforcement organizations on test results, resulting in immediate improvements in the tested products.

By improving the tools used by the law enforcement community and proving their effectiveness to third parties, ITL is making an impact in computer forensics. Our tools will reduce the time it takes for law enforcement to analyze seized computers or media and will provide confidence in the analysis of evidence presented in court. Our contributions to the improved efficiency and effectiveness of law enforcement will profoundly affect the nation. The websites are *http://cftt.nist.gov and http://nsrl.nist.gov.*

ELECTRONIC COMMERCE (EC)

ITL works with industry to develop standards, measurements, and reference implementations to ensure EC growth and use by all, including small- and medium-sized enterprises and individual users. We achieve this goal through several efforts and products. We develop conformance test suites for XML technologies and for Interactive TV (ITV) specifications, which provide developers and users with the necessary metrics to determine whether a particular implementation or application is conformant to a specification. Conformance is a recognized way to increase the likelihood that software products and applications are implemented correctly. We are also developing specifications and implementations for metadata descriptions and registries that will enhance the means by which information is defined, discovered, and retrieved. The development of reference implementations, prototypes, and conformance tests for ITV applications and XML registries for ebXML, circuit board supply chain (Internet Commerce for Manufacturing or ICM), EPA, and XML.gov will also help to enable and advance EC. These reference implementations and prototypes will help to find ambiguities and/or inconsistencies in the specifications, will be used for conformance testing, and will serve as models upon which other implementations can be built.

Andrew McCaffrey and Michael Koo create a videotape containing NIST Interactive TV Conformance Tests for the Declarative Data Essence Standard of the Society of Motion Picture and Television Engineers.

In FY2001, we released the XML Test Suite, Second Edition (+2000 tests), DOM Level 1 Test Suites, and partial test suites for XSLT, XSL-FO, and Schema. We developed a portal (roadmap) to EC standards that allows dynamic views. We authored conformance statements for ebXML, DASE, OASIS, and Government Smart Card specifications. We developed an OASIS and ebXML Registry information model and specification, as well as a Registry reference implementation and Registry conformance tests. We developed an ICM and Learning Object prototype registry. We served as a catalyst and contributor to the development of XML.gov and EPA registries. We provided tests and helped to develop standards for Interactive TV, including tests for the Declarative Data Essence (DDE) Group of the Society of Motion Picture and Television Engineers (SMPTE), a DDE reference application, and a Java™-based, educational application for the Digital Application Software Environment Committee (DASE), within the Advanced Television Standards Committee (ATSC). Finally, as part of our effort to harmonize our conformance testing work with the international community, we participated in the ITU JRG1 standards harmonization effort and served as the Editor of ISO/IEC 11179 Part 5 and Procedures for Achieving Data Registry Content Consistency.

By enabling and advancing EC, ITL is making a substantive impact. We are improving the quality of XML and EC specifications and implementations, thereby promoting portability and interoperability. Distributed, interoperable registries enable information exchange among marketplaces. Finally, we enhance the ability of the EC community to grow their businesses by facilitating information interchange and the creation of business alliances in the world marketplace. The website is *http://www.itl.nist.gov/div897/*.

HEALTHCARE

The Department of Veterans Affairs (VA) asked ITL to help them assess new information technologies for application to their hospitals. Since the initiation of this effort, ITL has participated in the development of healthcare information technology standards, such as the Resource Access Decision (RAD) Facility in the Object Management Group (OMG) and the G-8 Healthcare Data Card Project. We strive to improve the quality of healthcare information systems by designing distributed models and architectures for healthcare information systems, developing reference implementations for these models and architectures, and participating in the development of standards for healthcare information systems. A significant aspect of this project is technology transfer of NIST Role Based Access Control (RBAC) work.

In FY2001, we developed the Remote Procedure Call Broker to automate access to patient records. We

Len Gallagher and Michael Kass discuss their development of the XML Registry information model and prototype for electronic commerce applications.

designed and implemented the Inter-Organizational Role Based Access Control (IORBAC) authorization mechanism. We designed and deployed the Enterprise Single Sign-On (ESSO) to all VA hospitals. The OMG RAD Facility was formally adopted as an OMG Specification. We are also collaborating with 2AB Inc. to apply RAD to the VA environment.

Our impact in these healthcare efforts has been significant. We made significant contributions to the VA moving patient data access from a manual to an automated system, while, at the same time, designing and implementing authorization and authentication mechanisms. ITL designs and implementations are a permanent part of the VA Health Information Systems Architecture, and NIST is a permanent consultant to the VA Architecture Design Group. Our contribution to the OMG RAD Facility is prominently acknowledged in the specification, which is being processed as an ISO and ASTM standard. The website is *http://www.nist.gov/va/*.

RESEARCH TO IMPROVE TESTING

Software testing improves software quality. Up to 50 percent of the cost of software development is testing. Writing tests is expensive, labor-intensive, and time consuming; consequently, developers often skimp on testing. Software testing also reduces vulnerabilities that can be attacked by hackers.

The goal of this ITL project is to improve the science of software testing and measurement. The project focuses on the application of formal methods and statistical methods to improve software quality. We are harnessing formal methods to improve the quality of software by automatically generating tests for software from formal specifications, thereby reducing costs. Deriving tests from specifications is particularly useful for bodies developing software standards, e.g., W3C, OMG, IEEE, and ANSI. Our project furthers software quality by companies implementing software, based on specifications, by providing a method to generate software tests that are automatically run to determine whether the software conforms to its specification. Quantifying software by applying statistical methods to software testing is another area of research.

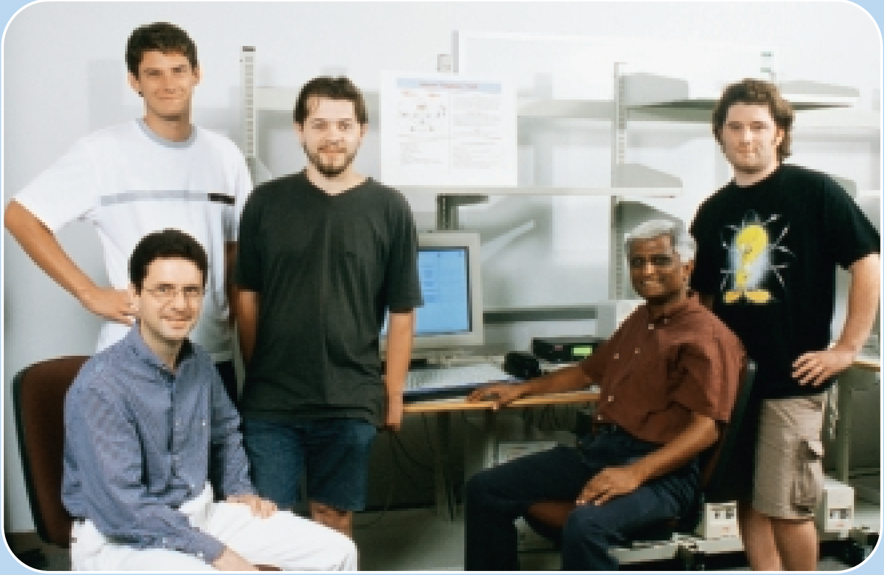
In FY2001, we developed a method and reference implementation to automatically generate tests and a coverage metric to support the method. We developed a new mutation engine for automated test generation. We developed intermediate representation (in XML) to translate between formal languages. We formed an intermediate representation group with industry and academia to standardize the NIST intermediate model. Using statistical methods, we developed a method to quantify results of conformance tests and a second method to test and validate object-oriented software. We worked with the standards organizations, W3C and OASIS, to apply methodologies and incorporate techniques into specifications, test design, and development. Finally, we developed methods to test and validate object-oriented (OO) software via automated techniques. Our work is making a significant difference as software products with fewer failures and closer adherence to standards come to the market earlier and at less cost. The website is *http://www.itl.nist.gov/div897/*.

NETWORKS

AGILE SWITCHING INFRASTRUCTURES

In response to industry needs to develop standards for an integrated Internet and optical network infrastructure, ITL has expanded its agile switching project to include testing and analysis of competing technical approaches in this area. Our initial focus was on integrated control planes for optical switched networks and dynamic control algorithms for traffic engineering and fault tolerance. In FY2001, we released a research prototype of G-Multi-Protocol Label Switching (MPLS) signaling protocols. We completed the design and implementation of a simulation framework for MPLS/optical switching infrastructures. We contributed comparative evaluations of integrated routing and signaling protocols to the Internet Engineering Task Force (IETF) and the Optical Internetworking Forum (OIF). In the fault tolerance area, we analyzed and reported results on potential modes of attacks on optical transport networks and their potential detection and recovery schemes. Working with George Washington University, we also implemented optical network restoration algorithms on our optical network-modeling tool called MERLiN.

Our work impacts the industry by improving the quality and timeliness of interoperable standards for integrated MPLS/optical signaling protocols and control systems. Our contributions of rapid prototypes and modeling and analysis tools benefit industry and academic researchers working on the next-generation optical Internet. The website is *http://w3.antd.nist.gov/agile_switch.shtml.*



Olivier Deruelle, Marc Bednarek, Christophe Chazeau (standing), Tim Hall and Mudumbai Ranganathan (seated) work on future optical networks.

DEVELOPMENT OF STANDARDS FOR WIRELESS PERSONAL AREA NETWORKS

ITL researchers are working with industry to promote the development of cost-effective, interoperable, and secure protocols for networking of pervasive computing devices. One research project involves working with the Institute of Electrical and Electronic Engineers (IEEE) standards group IEEE 802.15 to standardize Wireless Personal Area Network (WPAN) technologies, and we have made significant contributions to the IEEE 802.15's work.

WPANs are essentially cable replacement technologies that allow closely located digital devices to exchange information. Most technologies considered for WPANs, such as Bluetooth* and HomeRF™ employ an unlicensed radio frequency band in the range of 2.4 GHz (the so-called Industrial, Scientific, and Medical, or

ISM, band). This same frequency range is also used by existing standards for Wireless Local Area Networks (WLAN), for example IEEE 802.11. As the number of technologies using the ISM band increases, concern arises about the possibly deleterious effects of mutual electromagnetic interference. Designing wireless protocols that can share this scarce spectrum presents a key challenge in the design of WPANs.

ITL's efforts focused on: (1) modeling and validation of the Bluetooth* protocol specifications, (2) assessment of interference among wireless devices operating in the 2.4 GHz band, and (3) development and evaluation of coexistence mechanisms for wireless devices sharing the same spectrum. ITL researchers led the effort within the IEEE 802.15 Task Group on Coexistence to study and quantify radio-frequency interference between Bluetooth* and WLAN devices. In addition, ITL researchers proposed mechanisms and technical solutions to allow these devices to coexist when operating in close proximity. Contributions by ITL researchers were adopted by the IEEE 802.15 as the basis for a recommended practices document on coexistence that will be published in 2002. The website is *http://w3.antd.nist.gov/net_pc.shtml.*

INTERNET INFRASTRUCTURE PROTECTION

ITL works with the Internet Engineering Task Force (IETF) community to improve the scalability and performance of integrated Internet security systems and to expedite the development of Internet infrastructure protection technologies. The project originated from a request by the IETF directors and the Department of Defense for ITL to collaborate with key industry partners to ensure the timely development of Internet security technologies.

In FY2001, we released expanded reference prototypes and test systems to include advanced authentication and interfaces to Public Key Infrastructure X.509 (PKIX) systems. We developed benchmarking/ management tools for Domain Name System (DNS) Security (DNSSEC). We published simulation analysis of the scalability of Internet Protocol Security (IPsec) / IKE / PKIX in large-scale virtual private network (VPN) environments. Finally, we contributed to the design of IETF security policy management protocols.

ITL is advancing the crucial area of Internet infrastructure protection by leading the development of IETF standards for DNS security. Our rapid prototypes and online test systems assist industry in the testing of early product developments. Through the release of simulation tools, we facilitate the work of industry and academic researchers in the evaluation of the scalability of emerging IETF security systems. The website is *http://w3.antd.nist.gov/ iipp.shtml.*

David Cypher, Nada Golmie, and Robert Van Dyck perform modeling and evaluation of wireless personal area networks protocols.

Eun-Hyuk Lim, Kwang-il Lee, Mark Carson, Richard Rouil (standing), Oliver Borchert, David Griffith, and Young-Tak Kim (seated), members of the Agile Switching Infrastructures Project, are researching integrated, multilevel control and signaling protocols for next-generation optical Internets.

WIRELESS AD HOC NETWORKS

This ITL project responds to the needs of industry organizations, such as the Internet Engineering Task Force (IETF), and government agencies, such as the Defense Advanced Research Projects Agency (DARPA), for standards and protocols for wireless mobile ad-hoc networks (MANETs) that enable communication among autonomous collections of mobile users and distributed sensors. We work with industry, academia, and government to facilitate the development of technology and standards for MANETs and smart sensor networks.

To accomplish this work, we are investigating methods for implementing priority access and messaging for MANETs. We developed an OPNET evaluation platform for MANETs, including models for the Dynamic Source Routing (DSR) and Ad Hoc On Demand Distance Vector (AODV) protocols. We developed analytical techniques for validating simulations. We improved the convergence behavior of an optimal distributed detection algorithm, thereby lowering the probability of interception. In addition, we extended distributed detection/estimation algorithms to provide robustness for use in wireless sensor networks.

ITL's impact is significant. Industry benefits from our assistance in the design and analysis of protocol standards for routing in mobile ad-hoc networks. Research communities utilize our contributions to define models and algorithms for self-organizing networks. Finally, we are building a competence that positions NIST to become a major contributor to the development of next-generation wireless ad-hoc networks. The website is *http://w3.antd.nist.gov/wctg/manet/manet2.html*.

INFORMATION ACCESS

NIST Meeting Room Data Collection photos taken simultaneously with multiple cameras during a focus group discussion. Pictured are (clockwise from bottom left) Mark Przybocki, Elham Tabassi, John Garofolo, Vincent Stanford, Alvin Martin, Martial Michel, and (in lower view) Jonathan Fiscus.

HUMAN LANGUAGE TECHNOLOGY

ITL is developing and applying metrics and testing to advance the state of the art of human language processing, including speech and speaker recognition, spoken language understanding, information search, retrieval, and filtering, and other advanced text processing techniques such as summarization and extraction. This work also increases communication and technology transfer between industry and academia in the field of human language technology. To meet these goals, we are developing measurement methods and evaluation infrastructure, providing reference materials, including test data, coordinating community-wide benchmark tests within the research and development community, and building prototype systems.

This program is composed of several major projects, including automated speech recognition (ASR), the Text Retrieval Conferences (TREC), Topic Detection and Tracking (TDT), Automatic Content Extraction (ACE), and the Document Understanding Conferences (DUC). Since the mid 1980s, NIST has been developing the test protocols and speech corpora for the training, development, and evaluation of ASR technologies. Since 1998, NIST has produced over 250 speech corpus CD-ROMs. NIST has continued to advance the state of the art in spoken language technologies by focusing its benchmark tests on ever-more-difficult domains such as the recognition of broadcast news recordings in several languages. In FY2001, we conducted the NIST speaker recognition evaluation with 12 participating sites. We also conducted the NIST conversational telephone speech recognition evaluation with 8 participating sites. We provided test participants for DARPA Communicator trials and analyzed results. We also created a data collection facility for the automatic meeting transcription project and initiated work on software tools infrastructure.

The annual TREC conference series began in 1992 to advance the state of the art of text-searching technologies, such as document retrieval and question answering. Through TREC, NIST provides a vehicle by which the broader text retrieval community can participate in metrics-based evaluation of these technologies. In FY2001, we performed evaluation and analysis of data for text retrieval of web information and presented results at TREC-9, which was organized and hosted by ITL. In the area of question answering, we created a test collection and queries for testing the retrieval of answers rather than documents. We led the English portion of the

European Union's 2001 Cross Language Evaluation effort. We performed evaluation and analysis of cross language text retrieval using English and Chinese. We administered the Topic Detection and Tracking 2000 evaluation and performed analysis of evaluation results.

ITL also participates in the Document Understanding Conference (DUC), which is part of a DARPA project called Translingual Information Detection, Extraction, and Summarization (TIDES). Following an organizational meeting in November 2000, the first evaluation meeting took place in September 2001.

ITL's work is resulting in industry's improving web information retrieval performance in next-generation search engines. We are improving the capability to answer complex questions from information on the web (as opposed to just retrieving documents), to retrieve documents in other languages, and to transcribe telephone speech, as well as improving interactive telephone speech processing. We are also increasing the availability of test collections (for document retrieval, filtering, speech recognition, speaker recognition) to the research community for further improvements, facilitating the cross-fertilization of ideas across research groups, and launching new research areas by providing necessary evaluation infrastructure. The websites are *http://www.nist.gov/speech/* and *http://trec.nist.gov.*

Ellen Voorhees, Donna Harman, Paul Over, and Ian Soboroff design the next series of evaluations for the NIST Text REtrieval Conference (TREC).

INTERACTION AMONG USERS AND INFORMATION

ITL is providing metrics, standards, and test methodologies to improve interactive systems by developing standard usability reporting formats, new approaches and benchmarks to support usability testing, especially for the web, test methods for accessibility, and advanced user interface prototypes.

In FY2001, we completed and released Version 2.0 of the NIST Web Metrics software, and we upgraded the WebSAT and WEBVIP tools. We organized and hosted the fourth workshop on pilot testing of the Common Industry Format (CIF) and submitted it to the National Committee for Information Technology Standards (NCITS) as a fast track standard; the standard was approved on November 15, 2001. We distributed a CD for the purpose of pilot studies on CIF Testing, Evaluation, and Reporting (CIFter). We initiated development of an evaluation methodology and toolkit for usability evaluation of complex information management applications. We participated in the NCITS V2 standards committee to develop an alternative accessible interface protocol. We organized and hosted a successful IT Accessibility Conference at NIST in May 2001. We also hosted a Usability Professional Association (UPA) Workshop on Evaluation and Measurement for Accessibility.

As a result of this program, a standardized reporting format will be available to help software procurers compare results of usability tests so they can make better purchasing decisions; it also provides usability testers with a standard means to report the results of their tests. The program will also help provide methodologies and a set of benchmarks for testing usability. In the near-term, there will be novel approaches available for evaluating the usability of websites; in the long-term, there will be new methodologies for evaluating the ever-changing web environment. Industry-developed standards for new interaction paradigms, such as the NCITS V2

Paul Hsiao, Joe Konczal, and Emile Morse pilot usability tests as part of the Common Industry Format (CIF) reporting project.

Alternative Interface Access Protocol, will provide a variety of new ways beyond keyboard input for users, especially people with disabilities, to interact with computers and other electronic devices; ITL will help provide the testing infrastructure to measure the usability of these new interfaces. The websites are *http://www.nist.gov/webmetrics/*, *http://www.nist.gov/iusr,* and *http://www.nist.gov/cifter.*

MULTIMEDIA TECHNOLOGY

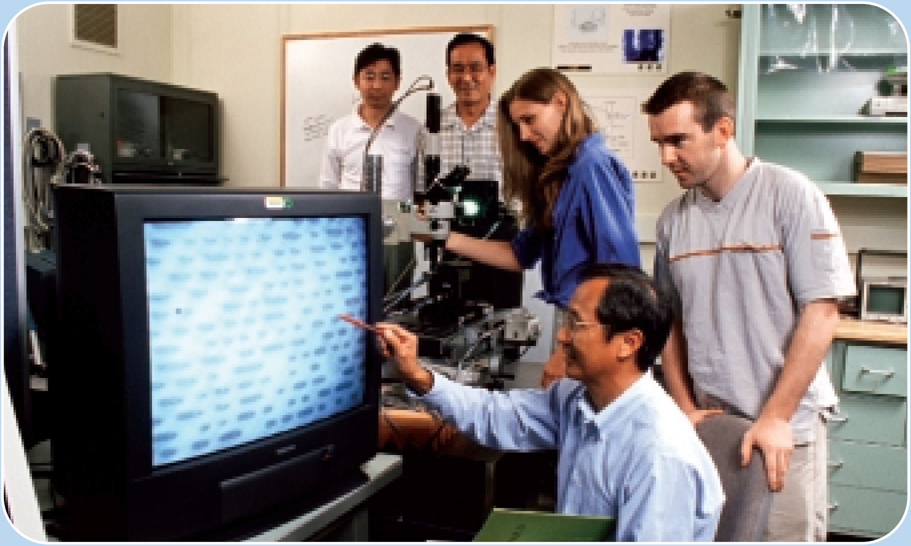
ITL is using metrics, standards, and testing to advance technologies for accessing and using multimedia information, including multimedia searching and filtering. We advance multimedia standards through leadership positions on standards committees (MPEG, JPEG, Web3D). We develop measurement methods for the evaluation of multimedia metadata (MPEG-7) for the purpose of content-based multimedia retrieval. We provide measurement and evaluation infrastructure to advance the technologies dealing with content-based access to audio-visual multimedia. We foster research in content-based retrieval from digital video and help ensure that encoders are MPEG-7-compliant by developing scoring software. Finally, we coordinate the development and establishment of a conformance and interoperability test bed to validate, enhance, provide for interchange, and benchmark the MPEG-7 technology.

In FY 2001, we continued to chair NCITS/L3 – U.S. Technical Advisory Group and delegation to ISO for the JPEG and MPEG international standards bodies, coordinating the MPEG and JPEG international meetings and maintaining the NIST online data site for MPEG and JPEG standards activities. In December 2000, ITL established NIST as the host for the online MPEG data repository and management information system for at least the next three years. We identified the needs and approaches for conducting conformance and interoperability tests for MPEG-7 technology. We participated with MPEG-7 XM and CE developers to validate and produce MPEG-7 reference software and test data, developed a web-based MPEG-7 validator to validate MPEG-7 DSs, Ds, and DDL, and integrated MPEG-7 XM reference software via plug-ins with Virage Toolkit to evaluate MPEG-7 DSs, Ds, and DDLs. We created WebChisel, a web-based tool based on Chisel (a VRML optimizer) open source. Finally, ITL staff served as Vice President and on the Board of Directors of the Web3D Consortium, playing a key role in organizing the Web3D 2002 Conference.

Our work is making a difference, helping to increase the availability of commercial products for retrieving multimedia in a flexible way, including content-based retrieval technologies for automatically indexing multimedia. We contribute to the research community in content-based retrieval from digital video, with ITL providing the evaluation infrastructure. We facilitate the coordinated effort within the MPEG-JPEG standards community in the domains of multimedia, including digital video, digital audio, virtual reality, motion and still images, synchronized sound and music, and associated technologies. The existence of an ITL-developed evaluation infrastructure will enable the industry to test, validate, enhance, provide for interchange, and benchmark MPEG-7-based technologies. We promote the wider availability and use of commercial products for 3D on the web. Finally, our ITL-developed tools for industry support and accelerate standards development. The websites are *http://www.itl.nist.gov/iad/894.02/projects/dv/dvr.html and http://ovrt.nist.gov/home.html.*

INFORMATION INTEGRATION

DIGITAL CINEMA QUALITY



Jian Zheng, Richang Lu, Tracy Comstock, Xiao Tang, and Oliver Slattery inspect results of NIST-developed environmental tests for the preservation of CDs and DVDs.

To help U.S. video/cinema producers and related industries by developing quality measurements for digital cinema, ITL is creating a digital cinema laboratory with software and hardware for digital cinema acquisition, compression, display, and storage. In cooperation with U.S. industry, we are developing measurements and test materials for assessing the contribution of compression and other system components to digital cinema performance. We disseminate recommended test clips through the Society of Motion Picture and Television Engineers (SMPTE) or other suitable organizations. Our customers are U.S. movie producers, studios, distributors, exhibitors, federal agencies, and equipment manufacturers in order to assure content fidelity and integrity.

As a result of industry input from ITL's Digital Cinema 2001 Conference (co-sponsored by the National Information Standards Organization) held at NIST in January 2001, we are developing a research program to develop video/image test patterns materials and test methods to be used by the movie industry for digital cinema applications. We are directing the development of SMPTE standard subjective test materials, accessible, high-quality materials for technology development and assessment. We worked with the movie industry in Hollywood to complete standard definition materials in 2001. Eighty industry standard patterns were developed and delivered for projection system characterization. These were used for MPEG digital cinema compression tests. High-definition digital cinema materials are in development. The websites for project information and for downloading the NIST Digital Cinema Test Patterns and Image Viewer are *http://www.itl.nist.gov/div895/isis/projects/digitalcinemaproject.html* and *http://www.itl.nist.gov/div895/products.html.*

DIGITAL DATA STORAGE

ITL's digital storage laboratory works with industry, government, and academia to support interoperability and reliability testing of optical disks, to provide the U.S. disk industry with standards, to improve the safe preservation of digital information, and to develop new technology for next-generation data storage. Projects include the development of CD/DVD disk drive software to check compliance to the Optical Storage Technology Association (OSTA) MultiRead specification, the development of a test bed to determine optical disk lifetime and performance in terms of aging and environmental factors, e.g., light exposure, and the determination of reliability and performance of various writable optical disk media types. We also initiated a study of advanced 3-D data storage technology, which is opening up a new generation of optical data storage.

Our work will result in standard testing procedures for optical disk reliability and lifetime. User demand will cause drives to become compliant to the MultiRead specification, as more users test their disk drives with the NIST CD Compliance Tester. Standards for storage and preservation of data on optical disk media will improve digital data storage for multimedia and other applications. The websites for project information and for downloading the NIST CD Compliance Test Software are *http://www.itl.nist.gov/div895/isis/projects/datastorageproject.html* and *http://www.itl.nist.gov/div895/products.html.*

ELECTRONIC BOOK TECHNOLOGY

ITL is developing guidelines and prototypes for the use of electronic content on eBooks and other devices, e.g., Braille Readers. We are developing a prototype tactile graphics display to read text and pictures, developing and documenting comparisons in eBook file formats, and exploring applications for eBooks. In FY2001, we facilitated the development of the Open eBook (OEB) specification v 1.0. We also assisted in the initial organization of the Open eBook Forum, the industry standards and trade organization for eBooks. Our Braille/eBook R&D efforts merited the prestigious national 2001 R&D 100 Award. We also initiated a partnership with Stanford Research Incorporated and the Army's Distance Laboratory, the Washington eLearning Forum. Finally we have developed a Linux platform viewer to examine OEB documents.

By producing guidelines for the development and use of interoperable content for multiple reading platforms, we are creating opportunities for all readers, including greater accessibility to digital content for the visually impaired. The websites are *http://www.itl.nist.gov/div895/isis/projects/ebookproject.html, http://www.itl.nist.gov/div895/isis/projects/brailleproject.html,* and *http://www.itl.nist.gov/div895/products.html.*

INTERACTIVE DIGITAL TELEVISION

ITL has been a catalyst for the approval of an interactive digital television standard. The Advanced Television System Committee (ATSC), an international industry consortium of more than 200 members consisting of broadcasters, content creators, software vendors, and equipment manufacturers, announced at their October 2001 meeting that the digital television (DTV) Application Software Environment (DASE) standard was approved. DASE is the North America middleware standard for broadcast interactive television. NIST and the DASE specialist group are developing these standards in advance of widespread use of digital television technology.

Mike Indovina, Rob Snelick, Alan Mink, and Barry Hershman (seated) view a simulation of an interactive digital TV session based on their NIST-developed reference implementation.

The NIST open reference implementation of the DASE standard provides application developers and consumer electronic manufacturers an application development environment and a basis for an interoperable Digital TV receiver implementation.

The NIST implementation was a deciding factor in the final approval of the DASE standards documentation. Because of the complexity and size of this forward-looking standard, industry participants requested that ATSC demonstrate that DASE was implementable. The ATSC membership voted, by a clear majority, that this requirement was satisfied by the NIST Procedural (Java™) Application Environment implementation and the Samsung Declarative Application Environment implementation.

Hai Tang, Alexandria Chambers, Monique Spencer, and Elizabeth Williams review a B2B portal testbed to simulate trusted e-commerce transactions.

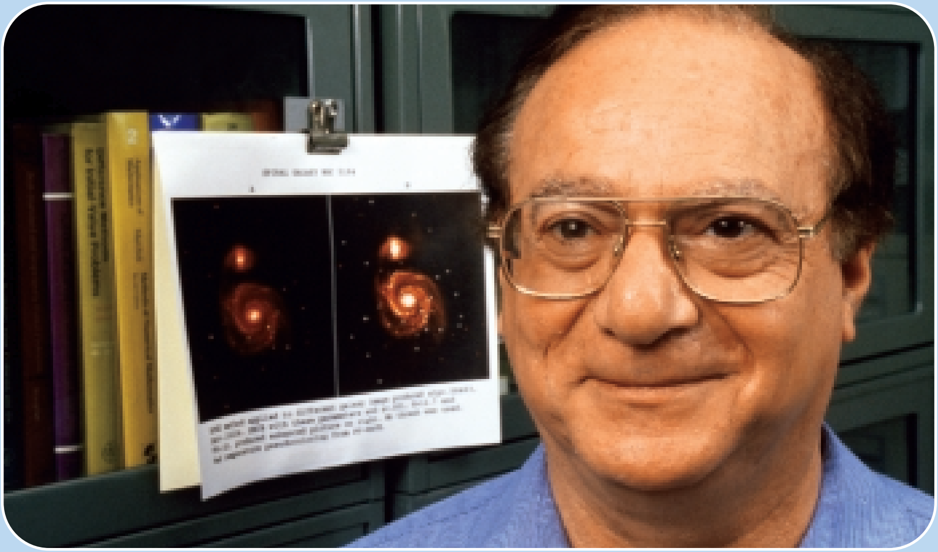
The interactive digital television community has been very responsive to the NIST prototype implementation. Over 800 copies of the software have been downloaded since its release, announced in June at the 2001 DASE Symposium held at NIST. Many key industry players such as Liberate Technologies, Insignia Inc., Panasonic, Sharp, and other ATSC member companies are early adapters of the NIST technologies. The NIST implementation is an enormous undertaking, consisting of over 100,000 lines of Java™ code. The NIST environment provides not only the DASE implementation, but also an ATSC DTV receiver simulation and DASE reference applications. This is a major accomplishment for the digital TV industry, as all analog transmission is mandated by the FCC to be digital in 2007. The websites for more project information and for downloading the NIST DASE Prototype Reference Implementation are *http://www.dase.nist.gov* and *http://www.itl.nist.gov/div895/products.html*.

TRUST MANAGEMENT

ITL seeks to expand business opportunities to the smallest of web enterprises, which constitute half or more of the marketplace. We are providing standards, guidelines, and measurement technology for inexpensive, interoperable third-party trust and assurance mechanisms for Internet business. We seek flexible, modular Internet trust architectures. Our projects address identity authentication, agreement assurance, and participant rights, privacy, and responsibilities. In FY2001, we released a Phase One Report on the Financial Agent Secure Transaction (FAST) assurance framework. FAST addresses e-commerce participants with concerns about valid identities for other web parties, characteristics being claimed, promised or contracted for (examples are payment guarantee, shipping reliability or rights of product use), and privacy for personal data and business marketing information. Finally, we implemented a test application server to explore IPC (Electronics Interconnection Industry consortium) information format needs.

Working toward the goal of a trustworthy Internet, our trust management efforts will contribute to the expansion of the digital products market, projected to grow 50 fold from 1998 to 2003, due to the benefits of interoperability. The website is *http://www.itl.nist.gov/div895/cmr/ecom/index*.

MATHEMATICS



Alfred Carasso has developed a unique highly efficient method for the blind deblurring of images. Blind refers to the fact that the cause of the blur is unknown. This technique is being applied to several applications of electron microscopy at NIST, but is widely applicable.

APPLIED MATHEMATICS

Ensuring that sound mathematical methods are applied in NIST research is a cornerstone of the ITL applied mathematics program. Working directly with NIST scientists and engineers, we develop requisite mathematical technologies, including mathematical models, methods, and software. Mathematical modeling provides a cost-effective alternative to experiments-based science and engineering, hence its growing use in industry. Within NIST, mathematical modeling is used as a complement to its experiments-based measurement program, allowing the analysis of measurement systems before and after experimental programs. This helps avoid costly delays and helps ensure success. One example is our development of a new method for blind image deblurring (i.e., deblurring when the cause of the blur is unknown). The technique is very fast and widely applicable. The new technique is in use in several projects in the NIST laboratories.

Our impact on NIST research and the larger scientific community is considerable. At NIST, we have successful ongoing collaborations in such areas as materials science, high-speed machining, and construction technology. Distribution of related methodology and tools, including computer software, allows these benefits to accrue to the scientific community at large. For example, we have developed widely used packages for modeling magnetic materials (OOMMF), as well as materials with complex microstructure (OOF). We also have direct connections to other agency programs relevant to NIST needs. For example, two of our researchers recently began a significant new multi-year Defense Advanced Research Projects Agency (DARPA) project on high-accuracy geometry representation and quadrature methods for computational electromagnetics. The website is *http://math.nist.gov/mcsd/*.

DIGITAL LIBRARY OF MATHEMATICAL FUNCTIONS (DLMF)

The goal of this ITL project is to develop an authoritative and comprehensive reference work on the special functions of applied mathematics. Such functions are extremely useful tools in mathematical and computational modeling in a very wide variety of fields. The effective use of these functions requires access to a convenient source of information on their mathematical properties, such as series expansions, asymptotics, integral representations, relations to other functions, methods of computation, etc. The DLMF will replace the outdated NBS Handbook of Mathematical Functions (AMS 55, 1964), presenting information in a freely accessible online, web-based, highly interactive, and visual format. The project is scheduled for completion in 2003.

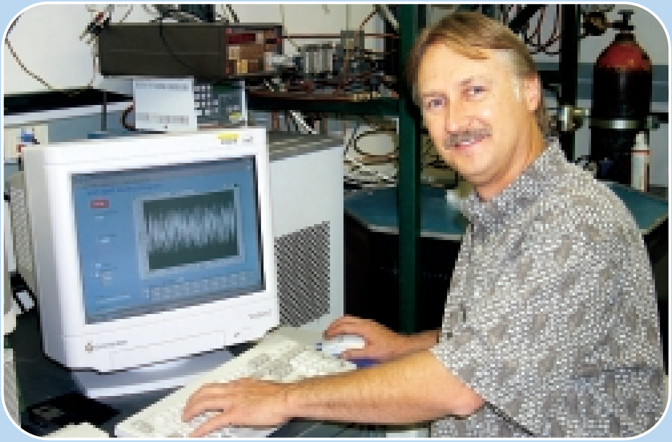
In FY2001, the DLMF project continued on schedule. External experts are generating most of the technical material for the DLMF. Contracts were issued for all 40 technical chapters, and first drafts were received for most. Many are now undergoing revision. Candidate validators for the technical data were identified. We also developed a prototype search capability for the online resource. External enthusiasm for the project remains high. The April 2001 issues of *Physics World* and *Physics Today* featured news articles on the DLMF. An expected benefit of the DLMF will be the standardization of notations and normalizations for the special functions, as well as enhanced traceability to NIST for standardized mathematical objects. The website is *http://dlmf.nist.gov/*.

Bonita Saunders (seated) works with students Brianna Blaser and Elaine Kim to develop graphics that illustrate the properties of standard functions of applied mathematics for the NIST Digital Library of Mathematical Functions.

HIGH PERFORMANCE COMPUTING AND VISUALIZATION

ITL collaborates with NIST scientists on the application of parallel computing and scientific visualization to mathematical models of physical systems. The most demanding computing applications require resources that far exceed those routinely found on a scientist's desktop. To perform such computations in a reasonable amount of time, one must often resort to the use of parallel computers. The effective use of such systems requires that algorithms be redesigned, often in fundamental ways. Effecting these changes, and debugging the resulting code, requires expertise and a facility with specialized software tools that most working scientists do not possess. We support the use of NIST's centralized parallel computing facility by providing expert consulting and collaboration in these areas. This work often leads to new tools of widespread use. This year, for example, working in collaboration with the NIST Materials Science and Engineering Laboratory, we developed a parallel version of the popular Feff code for X-ray absorption spectroscopy that runs 20-30 times faster than the original. Another example is the Interoperable Message Passing Interface (MPI) standard, which saw its first public demonstration by vendors at a major trade show this year.

The use of sophisticated visualization equipment and techniques is necessary to adequately digest the massive amounts of data that high-performance computer simulations can produce. ITL provides hardware and software tools to enable scientific discovery in large datasets of this kind. Effective use of these tools requires a great deal of expertise, and hence we work closely with NIST scientists to make effective use of them. In FY2001 for example, we achieved a series of extremely successful visualizations of the results of simulations of Bose-Einstein condensates in collaboration with the NIST Physics Laboratory, which were featured in *Physics Today*, *Optics and Photonic News*, and *Scientific American*. We completed the installation of the RAVE visualization environment, a system that enables three-dimensional immersive visualization, using stereo eyeglasses. A variety of applications from the NIST laboratories have been



Jim Filla provides support to a large number of scientists at the NIST Boulder Laboratories who are using LabVIEW to control and monitor measurement test systems and to collect, display, and analyze data. Here he is pictured with the Very-High-Temperature Guarded-Hot-Plate apparatus, used to make absolute thermal conductivity measurements on ceramics and ceramic coated super-alloys. Measurements made with this apparatus will be used to help establish international high-temperature thermal conductivity standards.

ported to the system. The website is *http://math.nist.gov/mcsd/savg/*.

MATHEMATICAL SOFTWARE

Mathematical modeling in the sciences, engineering, and finance inevitably leads to computation, the core of which is typically a series of very well defined, recurring mathematical problems, such as the solution of a differential equation, the solution of a linear system, or the computation of a transform. Much research has focused on how to solve such problems efficiently. The most effective means of passing on this expertise to potential customers is by encapsulating it in a reusable software component. Since much work at NIST relies on such computations, NIST has a natural interest in seeing that such components are developed, tested, and made available. ITL develops mathematical algorithms and software of this type in response to NIST needs. The computational science community outside of NIST has similar needs for programming methodologies. We also advance the development of standards for mathematical software tools and ensure widespread dissemination of research software, testing artifacts, and related information to the computational science community at large.

In FY2001, working with the Basic Linear Algebra Subprograms (BLAS) Technical Forum, we finalized the specification for the Sparse BLAS interface standard; a reference implementation is in process. We released the Zoltan dynamic load-balancing library jointly with Sandia National Laboratory. We worked with the Java™ Grande Forum, demonstrating the utility of Java™ for scientific computing with our web-based SciMark benchmark. Finally, we maintained the popular Guide to Available Math Software and Matrix Market web services. These services are available at *http://math.nist.gov/*.

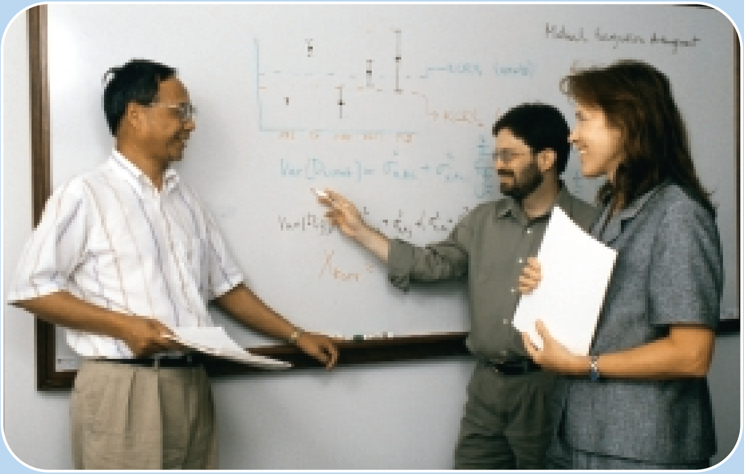
QUANTUM COMPUTING

ITL is working with the NIST Physics and Electronics and Electrical Engineering Laboratories to develop a measurement and standards infrastructure to support quantum communications, and to demonstrate and exploit new technologies for quantum computing. Quantum information networks have the potential of providing the only known provably secure physical channel for the transfer of information. The technology has been demonstrated only in laboratory settings, and a solid measurement and standards infrastructure is needed to move this into the technology development arena. Quantum computers have potential for speeding up previously intractable computations. We are supporting the work in the Physics Laboratory to develop quantum processors and memory, concentrating on the critical areas of error correction, algorithm and tool development, and information theory.

In FY2001, we began the development of an open, measurement-focused testbed facility for quantum communications for the DARPA Quantum Information Science and Technology program. This will allow a better understanding of the practical commercial potential for secure quantum communication and serve the development of standardized network protocols for this new communications technology. We developed a hybrid quantum authentication protocol for use on such networks. We are also collaborating with the NIST Physics Laboratory on the development of models of quantum gates, as well as on models of error propagation through arrays of gates representing quantum algorithms. Our website is *http://math.nist.gov/quantum/*.

STATISTICS

BAYESIAN METROLOGY



Nien-Fan Zhang, Will Guthrie, and Blaza Toman discuss potential uncertainty analyses for international interlaboratory studies between National Metrology Institutes known as Key Comparisons.

NIST statisticians are expanding fundamental statistical theory necessary to the specialized development and implementation of Bayesian methods for metrology. Important topics for metrology are traceability of measurements and the propagation of uncertainty, interlaboratory comparisons, calibration, scientific process modeling constrained by physical laws, and the development of a scientific basis for "uncertainty B." In FY2001, Bayesian methodology developed at NIST was used for the analysis of key comparison data for international laboratories. The development of both generic and specialized Bayesian hierarchical models for the "consensus mean" problem was followed by implementation. Adding these calculation tools to DataPlot makes this Bayesian analysis available to scientists at NIST and at other National Metrology Laboratories around the world. By way of example, this Bayesian methodology was applied to the estimation of the consensus means and the uncertainties for 88 compounds as part of the Standard Reference Materials (SRMs) Program. Graphical representations of Bayesian inferences are currently being developed, implemented, and prepared as web-based products for use by NIST scientists and those in the industrial arena. The website is *http://www.itl.nist.gov/div898/BayesMetrics/*.

KEY COMPARISONS AND INTERLABORATORY EQUIVALENCE

With the signing of the Mutual Recognition Agreement (MRA) by the National Metrology Institutes around the world, international interlaboratory key comparisons have taken on even greater importance in the NIST mission. These key comparisons serve as the technical basis for acceptance of measurements by the various member laboratories for purposes of commerce. The International Committee on Weights and Measures has developed an MRA that requires a measurement comparison mechanism that reflects accurately the true relationships between measurement systems maintained by its member laboratories. The results of these key comparisons must also be extensible to members of Regional Metrology Organizations to maximize recognition of measurement capabilities of other metrology laboratories around the world.

In FY2001, with three other NIST laboratories, we drafted an outline for collaborative research to define a consolidated approach to key comparisons. The use of key comparisons is increasing both in scope and in depth. ITL's experience with key comparisons in many different areas makes it a natural hub where design templates and analytic methodology for key comparisons can help ensure the success of the MRA to streamline measurement issues in international trade and measurement science. NIST statisticians also provide an international statistical resource for other metrology issues. With membership in the U.S. Technical Advisory Group for ISO/TC69 and as project leader for ISO/PDTS 21749, NIST statisticians provided an official review of the revision to ISO/Guide 35, *Certification of Reference Material-General and Statistical Principles*. The website is *http://www.itl.nist.gov/InterlabStats/*.

STATISTICAL ANALYSIS OF IT PERFORMANCE

Assessing quality in software, hardware, and networks draws on statistical models that are developed expressly for this purpose. At NIST, statistical modeling and research addresses these areas with major collaborative efforts in software testing, in information retrieval, in network performance assessment, and in ongoing work on standards for electronics. In FY2001, new methodology for algorithmic comparison was developed to provide statistical tools for comparing human identification system algorithms. This new methodology was based on using partial rank correlation methods together; other methods relied on analysis of variance and multiple comparisons techniques. The need for statistical evaluation of the reliability of conformance tests resulted in the construction of new methodology and its application to the NIST Computer Graphics Metafile (CGM) graphical conformance test suite. In a different venue, extension of multidimensional scaling methodology gives a more informative data analytic approach, leading to new insights to data from the Text Retrieval Conference (TREC). The website is *http://www.itl.nist.gov/div898/ITStats/*.

HumanID team members Kimball Kniskern, Susan Heath, Alan Heckert, Andrew Rukhin, and Stefan Leigh of the Statistical Engineering Division discuss ranking performance of algorithms for face recognition with (seated) Patrick Grother and Jonathon Phillips of the Information Access Division.

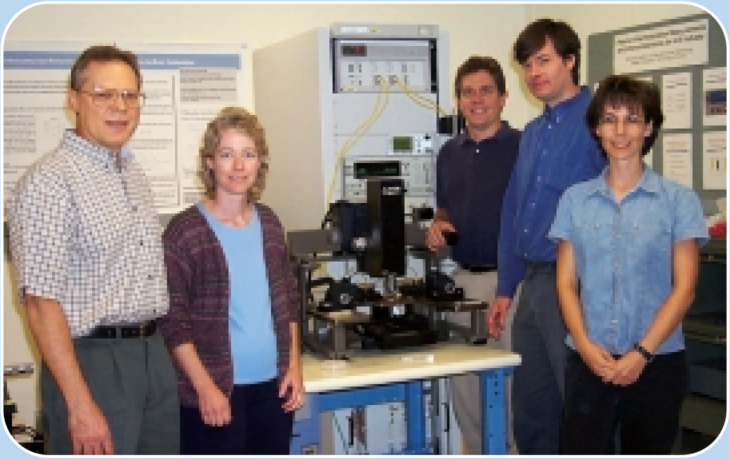
STATISTICAL COLLABORATIONS, MEASUREMENT

Measurement is the backbone for advancing scientific research and creating new technologies. Expertise in the design of experiments, process modeling, estimation of components of variance, quality control, and uncertainty analysis is coupled with a strong focus in applied research to bring ITL statisticians into contact with leading researchers in measurement science, both at NIST and elsewhere. Current advances in statistical methods for metrology, for modeling, for graphical data representation, for evaluation of uncertainty, and for data mining are used to support NIST research in physical science and engineering. Statistical metrology with uncertainty analysis, leading to certification, supports the Standard Reference Materials (SRMs) Program (60+ SRMs certified in FY2001) and NIST Calibration services. In FY2001, we implemented new methodologies for SRMs, including consensus mean code and Bayesian solutions. Research collaborations and general statistical consultation is provided to all the other laboratories at NIST; in FY2001 NIST statisticians from the Statistical Engineering Division collaborated with 79 percent of the other scientific research divisions at NIST.

Development of statistical measures can lead to adoption by industry, as in the case of measuring the sharpness of scanning electron microscope images. Statistical approaches to measurement and to comparison, the development and evaluation of test methods both in the laboratory and in the field, statistical experimental design and analysis, and optimizing experiment efficiency have recently been applied to products and/or industries as varied as paint, police body armor, electro-deposited coatings, magneto-resistive heads in computer disk drives, and integrated circuitry. The website is *http://www.itl.nist.gov/div898/StatServices/*.

STATISTICAL METROLOGY EDUCATION

ITL statisticians maintain an active series of courses taught at NIST, some of which are open to non-NIST scientists and engineers. Regular course offerings include Exploratory Data Analysis, Uncertainty Analysis, Experimental Design, Regression I & II, Analysis of Variance, Combining Information, Using Bayesian Statistics, and Analyzing Time Series Data. Additional courses on special topics are offered when demand is sufficient.



At the NIST Boulder Laboratories, Dom Vecchia, Kate Remley (EEEL), Don DeGroot (EEEL), Kevin Coakley, and Jolene Splett develop methods for characterizing nonlinear devices, components, and circuits used in digital wireless communications.

A significant joint project by NIST statisticians and SEMATECH is the development of a hyper-linked web document for constructing experiments and for analyzing data in order to improve and document measurement and production processes. This electronic Handbook is unique because readers access statistical software from within its pages to analyze either case studies in the Handbook or to reproduce analyses on other data. The Handbook updates the NBS Handbook 91, Experimental Statistics, and utilizes public domain software, Dataplot (developed at NIST), coupled with the case studies in the Handbook. Individuals can access the Handbook, for example, to follow instructions to construct a calibration curve from their own data. Alternatively, the Handbook can be used to implement training in design of experiments, analysis of data using linear models, or other topics. The electronic Handbook also interfaces with various commercial software packages. The website is *http://www.itl.nist.gov/div898/StatWebEd/*.

STATISTICAL PROCESS CHARACTERIZATION

ITL statisticians collaborate with NIST researchers and their industrial partners to characterize complex processes and to address measurement and standards aspects of physical science, engineering, and information technology. Current examples of process characterization include stochastic models for high-speed communications using optical fibers, new measurement methods for characterizing the complex permittivity of dielectric materials (widely used throughout the electronics, microwave, communication and aerospace industries), statistical models for polymer temperature and pressure measurement during fabrication, and characterization of high-speed oscilloscopes for use in optoelectronic device metrology, in nonlinear device metrology, and in high-speed digital circuit design.

This year we developed a procedure for estimating the electrical length and diameter of the microwave cavity in Dielectric Materials Measurement Systems, then determined the properties of the estimation procedure itself, and finally completed the uncertainty analysis. The NIST Kurtosis Program, developed by NIST statisticians as a multivariate kurtosis measure of SEM image sharpness measurement, has been implemented in the workstation designed by Spectal Company. Drawing on an underlying probabilistic model together with a statistical approach to data analysis, NIST statisticians developed a prediction model for Neutron Depth Profiling, both the energy spectrum for a material concentration profile and the theoretical stopping power. We also developed a procedure to adaptively estimate jitter and correct power spectrum of optoelectronic signals. The website is *http://www.itl.nist.gov/div898/StatModels/*.

SELECTED CROSS CUTTING THEMES

CRITICAL INFRASTRUCTURE PROTECTION

ITL is actively engaged in protecting the nation's vital infrastructures. American business and government operations rely directly and indirectly upon a national information infrastructure and supporting physical infrastructure, such as telecommunications, energy, financial services, water, and transportation sectors. Many of the systems and physical assets of these infrastructures are critical to the nation's security, economy, or health and safety. Information technology (IT) advances have caused these infrastructures to become increasingly automated and interlinked, creating new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks.

Consistent with its overall mission and long-standing security responsibilities in information technology, ITL focuses on security standards and testing to help ensure the security of our nation's critical infrastructures. We support federal departments and agencies under the Computer Security Act of 1987 and follow-on legislation that assign to NIST responsibility to develop security standards and guidelines for sensitive federal systems. We also help IT users and vendors build products that will protect information and improve security. (See the Security section of this report.) By working with IT vendors and users to develop security standards and security testing programs, ITL strengthens the security of commercial IT products, which provide the communications and information processing backbone of our infrastructures. By enhancing the confidence of the public, we enable more widespread and secure infrastructures supporting e-Government and e-Commerce.

A significant contribution to infrastructure protection is ITL's administration of the Critical Infrastructure Protection Grants Program. Congress established the program at NIST in response to the President's Committee of Advisors on Science and Technology (PCAST), which called for funding of significant critical information infrastructure protection research. The program funds research and development of new security solutions that are needed by the public and private sectors. Individual companies may be reluctant to pursue research in

CRITICAL INFRASTRUCTURE PROTECTION GRANTS FOR 2001

ORGANIZATION(S)	PROJECT TITLE
CygnaCom Solutions Inc., McLean, Va.	Engineered Compositions for Infrastructure Design
Decision Science Associates, Vienna, Va. and Lockheed Martin, Gaithersburg, Md.	Metrics and Tools for Evaluating Intrusion Detectors
Rether Networks Inc., Centereach, N.Y.	Compiler-Assisted Intrusion Detection/Prevention and Automated Damage Repair
Schweitzer Engineering Laboratories Inc. and Washington State University, Pullman, Wash.; and the University of Idaho, Moscow, Idaho	Industrial Applications of Information Security to Protect the Electric Power Infrastructure
Telcordia Technologies, Morristown, N.J.	Advanced Security Profiles and Enforcement for Next Generation Networks
University of California, San Diego, Calif.	Real-Time Intrusion Detection
University of Maryland, College Park, Md. and NAI Labs, Glenwood, Md.	Secure Wireless Infrastructure Test Bed
University of Pittsburgh, Pittsburgh, Pa.	A Survivable and Secure Wireless Information Architecture
University of Tulsa, Tulsa, Okla.	Vulnerability Analysis Tools and Attack Management Systems for Converged Networks

areas that are not cost-effective for them or that do not meet their unique market demands.

Industry and academic researchers are eligible to apply through a competitive evaluation process for the NIST grants. Proposals are evaluated based upon scientific merits, potential impact on future systems, and potential for technology transfer. To encourage the use of new technology, research results will be presented at a series of annual conferences open to government and industry. Grant topics may cover a wide range of areas, for example:

- Network system interactions and vulnerabilities to cascading effects;
- Robustness, resilience, and behavior of tightly coupled, complex, nonlinear systems;
- Design of "test beds" and other means for experimentally validating network security technologies;
- Fundamental principles, scientific basis, methodologies, and metrics for information assurance as an engineering discipline;
- Information assurance for emerging information technologies;
- Concepts for high-confidence systems and software;
- Increasing resistance to penetration;
- Next-generation intrusion and malicious code detection;
- User interfaces such as visualization of system security information;
- Self-healing systems;
- Security and forensics toolkits; and
- System architecture to ensure survivability, graceful degradation under stress, and ease of reconstitution.

In FY2001, the Critical Infrastructure Protection Grants Program funded nine research grants and awarded $5M. The website is *http://csrc.nist.gov/grants/index.html.*

"Computing has permeated our society -- in academia, business and government. We depend on our computing infrastructure for national defense, law enforcement, finance, medical care, communications, education and entertainment. Yet, despite its critical role, much of this infrastructure is built from software that was poorly designed and tested, connected using experimental protocols, and deployed based on lowest initial cost. This leaves us all in peril from criminals, vandals, and (especially) mistakes. Thus, it is gratifying to see NIST assert leadership and address important aspects of the critical infrastructure. It is an important initial investment in the public and private sector's Critical Infrastructure needs. I am confident that their choices will yield important results."

Eugene H. Spafford
Professor and Director
Purdue University Center for Education and Research
in Information Assurance and Security (CERIAS)

SELECTED CROSS CUTTING THEMES

PERVASIVE COMPUTING

ITL is pursuing a laboratory-wide pervasive computing initiative. This multi-faceted project is a natural fit for our organization, as we have robust research and development programs in human computer interaction, such as speech and visual recognition and tracking, sophisticated information access from multimedia databases, extensive information presentation capabilities, dynamic networking, wireless networking, software testing, and security.

Our approach is to define the necessary and sufficient conditions under which a system can be considered as pervasive, assess the suitability and applicability of current measurement techniques, develop new design and testing techniques to model and measure pervasive systems, and investigate integration and interoperability among sensors, devices, and computing components in a pervasive system. Specific projects include the development of new integration software to facilitate pervasive system experiments in industry, the analysis and evaluation of interference and coexistence techniques in the 2.4 GHz ISM band for pico-cellular wireless communication, and the development of tests and measures for dynamic service discovery.

College students Stephanie Gantt, Jennifer Quinn, Virginie Galtier, Alexandria Chambers, Peng Ying, Chris Brown, and Jack Hudson discuss their projects in ITL.

The goals of the pervasive computing initiative are to foster adoption of pervasive computing by providing industry, users, standards organizations, and academia with the tools and tests to identify and define product requirements. To accomplish this, we are developing, analyzing and comparing technical solutions, measuring components and systems, and developing high-quality, correct, robust implementations. We are also providing methodologies, metrics, tests, reference data, and technology.

To accomplish these objectives, we have been sponsoring a Pervasive Computing Conference series since 1998. We developed and released (open source) the

Students Virginie Galtier, Alexandria Chambers, and Peng Ying share their views on technology during their summer tenure at NIST.

NIST Smart Flow System -- an integration and interoperability software system. We developed a unique 59-element microphone array for speech data acquisition; we deployed the system and microphone array to the MIT Artificial Intelligence laboratory. We developed a "smart" projector prototype and benchmark test for the prototype. We developed Architecture Description Language models and performed an analysis of service discovery protocols. We developed a seven-layer conceptual model for defining pervasive computing with industry. We completed the EXiST Simulation Tool for modeling and measuring pervasive computing systems. We conducted measurements and performance evaluation of wireless devices (Bluetooth* and IEEE 802.11) in a coexistence environment. We developed behavior models and performance measurements for Jini™, Universal Plug and Play (UPnP), and Service Location Protocols (SLPs). We released benchmarking tools for service discovery protocols. We developed the software framework for simulation of large-scale, highly dynamic pervasive computing environments. Finally, we modeled adaptive control mechanisms for fault-tolerant service discovery.

Our contributions to industry in pervasive computing are expected to make a significant impact. Some examples are

- Establishment of the Smart Flow System as an interoperability standard for industry;
- Development of evaluation infrastructure for end-to-end integrated systems;
- Assistance to industry in the development of integrated smart space environments with multiple sensors, devices, and computers;
- Improvement of service discovery protocol specifications and metrics for comparison of the protocols;
- Simulation tool to facilitate requirements specification, modeling, and prototyping;
- Tools and measurements for performance and conformance;
- Software tools to create, manage, measure and test pervasive services and applications;
- Robust, correct, interoperable software and pervasive products;
- Support for industry to standardize technical mechanisms to facilitate coexistence among various technologies occupying the same unlicensed wireless frequency bands, thus enabling a rich and diverse market for portable pervasive computing devices;
- Assistance to industry in understanding the technical properties of the current (first) generation of dynamic service discovery and device configuration technologies emerging in industry, to better inform the design of the next and subsequent generations of such protocols; and
- Goal of positioning NIST to become a major contributor to the development of Internet 4.0.

The website is *http://www.itl.nist.gov/pervasivecomputing.html.*

ACCOMPLISHMENTS OF OUR SERVICES PROGRAM

BUSINESS SYSTEMS

ITL supports the NIST mission through the development and maintenance of central administrative applications (e.g., accounting, procurement, property, human resources). We continue to implement our Commerce Standard Acquisition Reporting System (CSTARS) project, with completion scheduled in FY2002. Our support for the Commerce Administrative Management System (CAMS) effort continues, with a FY2003 deployment date. As a result of our support for these critical services, NIST benefits from more secure, modern, and effective business systems. The website is *http://www.itl.nist.gov/div896/*.

CHIEF INFORMATION OFFICER (CIO)

ITL currently hosts the Office of the NIST CIO, which provides centralized business-level planning and program management for all NIST information technology resources and programs. This office administers for NIST the development of the NIST IT Strategic Plan, the NIST IT Operations Plan, and the NIST Systems Development Life Cycle (SDLC). The Office of the NIST CIO also oversees the NIST implementation of the governmentwide 508 Accessibility program. The 508 Accessibility program is intended to ensure that IT resources are available to all users. Also under development is an IT Architecture Plan for NIST, the specification for which is to be completed in early FY2002. The impact of this centralized management program is more consistent, business-focused information technology support within NIST.

The PC Support Team at the NIST Boulder Laboratories: Wendy Morrison (left front), Cathy Nicoletti, Reiner Teichmann, and Lisa Eldrige.

COMPUTER CENTER OPERATIONS

ITL provides central high-performance scientific computing resources and secure full-purpose data center facilities for all NIST scientific and administrative computer systems. Through central account management and resource allocation, we offer our NIST customers the benefit of cost-effective scientific computing and secure data center operations. The website is *http://www.itl.nist.gov/div896/*.

DESKTOP COMPUTING

ITL supports desktop computing resources throughout NIST. Projects include the implementation of a Central Help Desk and migration towards the Managed Desktop. Through these efforts, ITL ensures a more secure and effectively managed desktop computing environment. The website is *http://www.itl.nist.gov/div896/*.

E-NIST

The Government Paperwork Elimination Act (GPEA) requires all federal agencies to offer services to the public electronically, replacing paper and wet signatures with electronic/digital signatures and messages. With the e-Approval project, ITL initiated the process by first adopting digital signatures, electronic forms, and electronic routing for NIST internal use. This year we successfully implemented Travel Manager across NIST, which will save time and reduce costs. With the completion of e-Approval in FY2003, all NIST forms will be prepared electronically, with important information stored in a database, and then be electronically transmitted over the network for approval. Once the new internal electronic process is successfully implemented, ITL may extend the process of adopting electronic routing and digital signatures with other agencies and trading partners as part of a broader public key infrastructure (PKI). The result of e-Approval will be a more efficient, timely, and cost-effective paperwork approval process for the NIST staff, our customers, and industry partners.

Many of the e-NIST applications involve automating public business practices (e.g., web-based shopping carts). These applications have stringent security needs. With the implementation of e-NIST in FY2002, NIST will have a secure, integrated, and more unified architecture for supporting these applications and will minimize the risk these applications pose to internal NIST networks.

ENTERPRISE SERVERS

To meet the needs of the NIST staff for centralized server computing support, ITL operates and maintains the central NIST servers (e.g., e-mail, calendar, file servers, application servers). Ongoing projects include the centralization of e-mail accounts, NIST-wide Windows 2000 server administration, and NIST-wide directory architecture. Our centralized support results in more secure and cost-effective server administration for the organization. The website is *http://www.itl.nist.gov/div896/*.

IT SECURITY OFFICE

To respond to the increased security threats to computing resources and to adhere to all relevant federal policies concerning the implementation of agency security programs, ITL established the IT Security Office. This office assures the security of NIST computing resources, setting and approving policy for the NIST firewall, which repels hacker attacks and minimizes the effects of computer viruses. Through a variety of tools, techniques, training, and guidance documents, the IT Security Office provides the NIST staff with a more secure computing environment.

TELECOMMUNICATIONS

A reliable telecommunication system is key to the NIST mission. ITL operates and maintains the central NIST network and telecommunications facilities and provides for the NIST presence on the Internet. Through enhancements and upgrades, we strive to provide a more secure and effectively managed internal networking environment with increased capacity and connectivity. The website is *http://www.itl.nist.gov/div896/*.

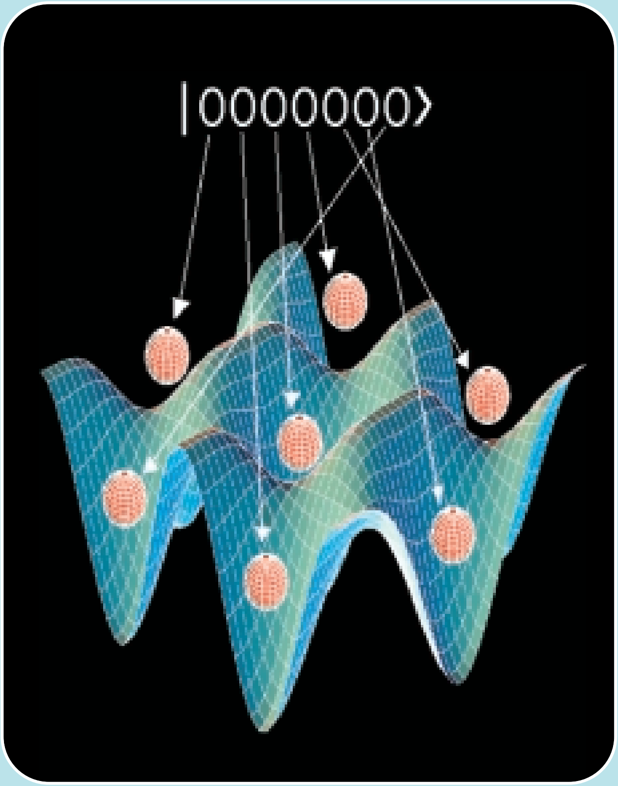
WEB

ITL operates and maintains the central NIST web servers and provides web consultation services to the NIST staff. To present a more visually appealing and effectively managed web presence, we are supporting the NIST laboratories as they implement a "One Face for NIST" on the web. The website is *http://www.itl.nist.gov/div896/*.

David Kao, Jeanne Springmann, Joe Kau, and Leslie Piwowarczyk (not pictured) design the database and web interface for the NIST KnowledgeNet.

INDUSTRY & INTERNATIONAL INTERACTIONS

ITL's research, measurement, and standards programs are greatly enhanced by our interactions with partners in industry, academia, government, and standards developers. In addition to four Cooperative Research and Development Agreements (CRADAs) with industry in FY2001, we participated in many consortia and industry interest groups, including the following:



ITL is developing software to optimize the use of qubits in quantum computing.

ADVANCED TELEVISION SYSTEMS COMMITTEE (ATSC)

The ATSC establishes voluntary technical standards for advanced television systems. ITL staff members Alan Mink, Robert Snelick, Wayne Salamon, Alan Goldfine, and Lynne Rosenthal participate in T3/S17, Digital TV Applications Software Environment (DASE) Application Programming Interface (API). ITL has been a catalyst for the approval of an interactive digital television standard.

AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI)

ANSI has served in its capacity as administrator and coordinator of the U.S. private sector voluntary standardization system for 80 years. Michael Hogan serves on the ANSI Information Systems Standards Board (ISSB), the Information Infrastructure Standards Panel (IISP), and the IISP Steering Committee. NIST/ITL is an ANSI-accredited standards developer. Michael McCabe is the contact for the ANSI/NIST-ITL 1/2000, Data Format for the Interchange of Fingerprint, Facial, & SMT Information standard.

ASSOCIATION FOR COMPUTING MACHINERY (ACM)

ACM is the world's oldest and largest educational and scientific computing society. John Barkley participates in the Role Based Access Control working group. Ronald Boisvert serves as Vice-Chair of the ACM Publications Board; he is the senior member of the Board, specializing in ACM's electronic publication program.

ASSOCIATION FOR INFORMATION AND IMAGE MANAGEMENT (AIIM) INTERNATIONAL

ITL participates in AIIM, the world's leading global association for information management professionals and providers of digital document technologies. Fernando Podio represents ITL on AIIM's Standards Board, as well as Committee C21, Advanced Data Storage Subsystems and two related subcommittees. Through our participation in AIIM, we facilitate the development of digital document standards worldwide.

ASTM

ASTM (American Society for Testing and Materials) is a not-for-profit 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, we promote quality in statistics.

BASIC LINEAR ALGEBRA SUBPROGRAMS (BLAS) TECHNICAL FORUM

The BLAS Technical Forum is an industry/government/academic working group, which is developing community standards for sparse matrix operations and extending the BLAS to new domains. Roldan Pozo chairs the sparse matrix subcommittee. Through participation in the forum, ITL contributes to the development of interface specifications and reference implementations for BLAS.

BIOMETRIC APPLICATION PROGRAMMING INTERFACE (BIOAPI) CONSORTIUM

The BioAPI Consortium is the federal government's focal point for research, development, testing, evaluation, and application of biometric-based personal identification and verification technology. Fernando Podio serves on the Steering Committee and the External Liaisons Working Group. Through this interaction, ITL supports the advancement of technically efficient and compatible biometric technology solutions on a national and international basis.

COMMON CRITERIA RECOGNITION ARRANGEMENT MANAGEMENT COMMITTEE

This group of 14 industrialized nations formed a cooperative agreement to recognize the results of security testing of IT products and systems conducted by accredited, independent, third party testing laboratories. Stuart Katzke serves as the Chairman of the Common Criteria Recognition Arrangement Management Committee Executive Subcommittee. ITL's leadership in this area has benefited both government and industry by increasing the availability of commercially tested IT products necessary to build more secure systems and networks for critical infrastructure applications.

CROSS INDUSTRY WORKING TEAM (XIWT)

The XIWT is a multi-industry coalition of information technology 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.

DIGITAL VERSATILE DISC (DVD) FORUM

The DVD Forum promotes the implementation and standardization of this data storage technology. Xiao Tang represents ITL on the Working Group on Data Format. Through our representation, we are contributing to a standard data format for DVD data storage.

ELECTRONIC BOOK EXCHANGE (EBX)

Providing intellectual property protection for the e-Book industry is the focus of EBX. ITL participates as a team member with technical support for the project. ITL chairs the authoring group for the Open e-Book Initiative, an industry group focused on developing a standard for electronic content on electronic book reading systems. We also participate in the Open e-Book Forum. Victor McCrary represents ITL in these efforts; he also serves on the Japanese Electronic Book Consortium Steering Committee. Through these interactions, ITL is advancing this important new technology.

FINANCIAL SERVICES TECHNOLOGY CONSORTIUM (FSTC) FAST WORKING GROUP

ITL participates with FSTC in its FAST (Financial Agent Secure Transaction) project. FAST addresses e-commerce participants with concerns about valid identities for other web parties, characteristics being claimed, promised or contracted for (examples are payment guarantee, shipping reliability or rights of product use, and privacy for personal data and business marketing information. Gordon Lyon represents ITL. Our support promotes economical trust and assurance for e-Commerce.

FORUM ON PRIVACY AND SECURITY IN HEALTHCARE

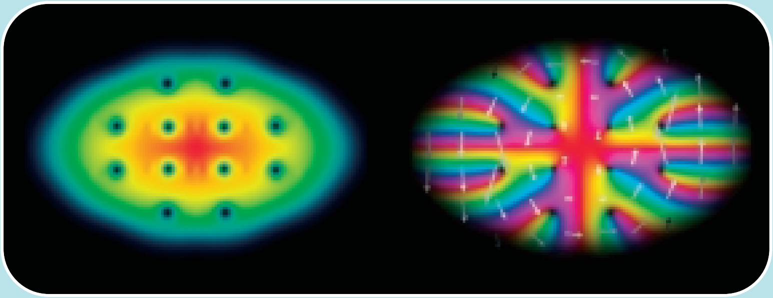
Sponsored by the National Information Assurance Partnership (NIAP) (a joint National Institute of Standards and Technology and National Security Agency initiative) and the Healthcare Open Systems and Trial (HOST), the forum is incorporated as a nonprofit charitable organization consisting of participating 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.

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. Xiao Tang represents ITL, which provides a neutral platform to perform testing and development that makes it possible for the industry to improve the interoperability and performance of their products for the increased demands for high-density data storage.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

IEEE is 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. David Cypher, Robert Van Dyck, Nada Golmie, and Nader Moayeri participate in IEEE 802.15, Working Group for Wireless Personal Area Networks, and Nader Moayeri also attends IEEE 802.16, Working Group on Broadband Wireless Access Standards. Finally, Larry Reeker 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.



Two renderings of a Bose-Einstein condensate containing quantized vortices. The left image shows the condensate density, where brightness and color are proportional to the number of atoms; the vortices appear as dark spots. The right image shows the phase (color) and the superfluid flow field (arrows).

INTERNATIONAL FEDERATION FOR INFORMATION PROCESSING (IFIP)

ITL participates in the IFIP Working Group on Numerical Software (WG2.5), which is part of the IFIP Technical Committee on Programming Languages (TC 2). The aim of WG2.5 is to improve the quality of numerical computation by promoting international cooperation in the development of languages, guidelines, tools, and standards for numerical software. Ronald Boisvert chairs WG2.5

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)

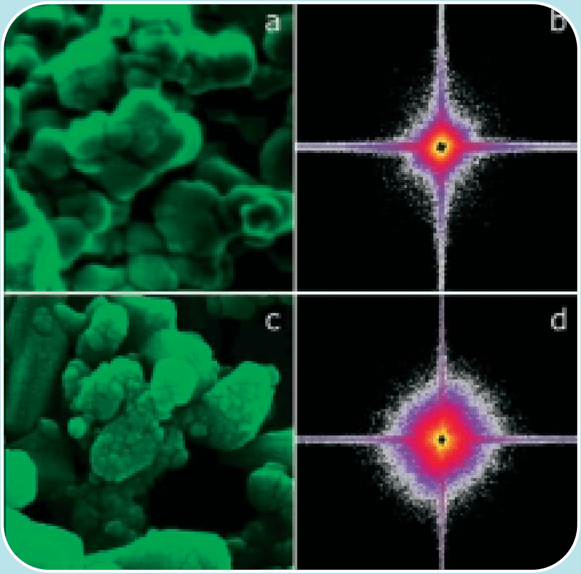
The ISO is a worldwide federation of national standards bodies from some 140 countries, one from each country. Nien-Fan Zhang serves on the Committee on Reference Materials WG1 for ISO Guide 35. Zhang and Nell Sedransk participate in the management group for Statistical Methods. Our contributions facilitate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

INTERNET ENGINEERING TASK FORCE (IETF)

ITL contributes to the technical development of the Internet through participation in the Internet Engineering Task Force (IETF). The IETF 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, Doug Montgomery, and Nader Moayeri participate in the Routing Area; Okhee Kim, Doug Montgomery, Sheila Frankel, Nelson Hastings, and Tim Polk participate in the Security Area; and Doug Montgomery and Mudumbai Ranganathan participate in the Transport Area.

INTERNET SOCIETY (ISOC)

The Internet Society provides leadership in addressing issues that confront the future of the Internet. It is the organizational home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). Doug Montgomery represents ITL. Our participation ensures that ITL has a voice in the next generation of the Internet.



The pictures illustrate scanning electron microscope (SEM) images of a heavily gold-coated oxide test sample, on the left, and their two-dimensional Fourier frequency magnitude distributions, on the right. A statistical measure of SEM image sharpness has been developed in terms of the multivariate kurtosis of the 2D spatial spectrum of the image.

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.

JAVA™ GRANDE FORUM

The Java™ Grande Forum (JGF) is an open working group of industrial, government and academic researchers, and software developers interested in improving the Java™ language and environment for technical computing applications. Roldan Pozo and Ronald Boisvert co-chair the Numerics Working Group, which has worked with Sun Microsystems to implement changes in Java's specifications which admit much faster execution (up to ten times faster) for computing-intensive applications.

JTC1 TAG

The Joint Technical Committee 1 (JTC1) develops, maintains, promotes, and facilitates IT standards required by global markets meeting business and user requirements concerning the design and development of IT systems and tools. Michael Hogan represents ITL on the U.S. TAG to ISO/IEC JTC1 on Information Technology, ensuring that ITL has a voice in global IT standards development.

MICROMAGNETIC MODELING ACTIVITY GROUP (muMAG)

muMAG 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.

NATIONAL COMMITTEE FOR INFORMATION TECHNOLOGY STANDARDS (NCITS)

NCITS's mission is to produce market-driven, voluntary consensus standards in a wide range of IT areas. Michael Hogan serves on the NCITS Policy and

Procedures Committee. ITL technical staff participate in many working groups, including multimedia and hypermedia information, MPEG development, still image coding, data representation, open distributed processing, IT security techniques, IT access interfaces, and e-Commerce. Through these interactions, we contribute our expertise to the development of IT industry standards.

NATIONAL INFORMATION ASSURANCE PARTNERSHIP (NIAP)

NIAP is a NIST/NSA partnership for testing methods and measures to ensure the quality of information security systems. ITL's Ronald Ross serves as Director of NIAP. Our involvement helps to ensure that the security testing needs of federal and industry IT consumers and producers are met.

NORTH AMERICAN OPEN MATH INITIATIVE

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

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, HTML, and CGM as well as others that are related to structured information processing. Mary Brady, Lisa Carnahan, and Lynne Rosenthal represent ITL; Brady chairs the conformance working group. ITL's participation includes the development of conformance tests for these standards.

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. Elizabeth Fong participates in the Business Object Management group. John Barkley is ITL's principal representative to OMG.

OPEN GROUP

The OPEN GROUP focuses on the development and implementation of a secure and reliable IT infrastructure. Shu-Jen Chang participates in Security Services.

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 represents ITL.

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.

PARALLEL TOOLS CONSORTIUM (PTOOLS)

Ptools brings together representatives from the federal, industrial, and academic sectors to address the factors that inhibit tool use and tool usability on parallel computers. Gordon Lyon represents ITL.

REAL-TIME JAVA™ EXPERT GROUP

The Real-Time Java™ Expert Group operates under the Sun Microsystem™ Open Community Process. Composed of industry representatives, the group is creating a standard for real-time extensions for the Java™ platform. Alden Dima represents ITL on the expert group, which bases its work on ITL's publication, *Requirements for Real-Time Extensions for the Java™ Platform*.

ROSETTANET eBUSINESS STANDARDS CONSORTIUM

Founded in 1998, RosettaNet is an independent, self-funded, nonprofit consortium dedicated to the development and deployment of standard electronic commerce interfaces to align the processes between IT supply chain partners on a global basis. Thomas Rhodes represents ITL.

SMART CARD SECURITY USERS GROUP (SCSUG)

Organized in 1999 under the sponsorship of NIAP, the SCSUG develops and promotes the use of standardized security requirements to ensure that the device security and data protection needs of the smart card end users are appropriately represented and met in smart card products. The SCSUG is composed of the major worldwide credit card brands (financial payment systems): American Express®, Europay, JCB, MasterCard®, Mondex™, and Visa®. Stuart Katzke represents ITL.

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. John Barkley, Andrew McCaffrey, and Michael Koo participate on the Committee on Data Essence Technology. Randall Easter attends the Study Group on Conditional Access for Digital Cinema. Charles Fenimore represents ITL on the Video Quality Experts Group.

STANDARDS COMMITTEE T1, TELECOMMUNICATIONS

Committee T1 is sponsored by the Alliance for Telecommunications Industry Solutions and accredited by the American National Standards Institute to create network interconnections and interoperability standards for the U.S. David Cypher and David Su participate; Su also attends T1X1, Digital Hierarchy and Synchronization. Through these efforts, ITL helps to ensure the interoperability of telecommunications systems in the U.S.

U.S. BIOMETRIC CONSORTIUM

The Biometric Consortium serves as the U.S. Government's focal point for research, development, test, evaluation, and application of biometric-based personal identification/verification technology. Fernando Podio participates in the Common Biometric Exchange File Format group. ITL was instrumental in the development of this standard.

VIDEO ELECTRONICS STANDARDS ASSOCIATION (VESA)

VESA promotes and develops timely, relevant, open display and display interface standards, ensuring interoperability and encouraging innovation and market growth. John Roberts represents ITL on four committees in this organization. As a member of VESA, ITL participates in the technical development of standards and develops laboratory implementations of proposed interface architectures.

To determine the viability of gait as a biometric, NIST collaborated with University of Notre Dame and University of S. Florida to stereoscopically capture 100 individuals walking an elliptical course on video. The database allows the effect of walking surface, shoe type, and load on gait to be studied. The images show a subject on concrete and grass with and without briefcase, view from two angles.

WEB3D CONSORTIUM

The Web3D Consortium provides an open 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.

WORLD WIDE WEB CONSORTIUM (W3C)

The W3C is an international industry consortium created to lead the World Wide Web to its full potential by developing common protocols that promote its evolution and ensure its interoperability. Mark Skall serves on the Advisory Committee. ITL staff members serve on a host of committees within this organization, including the Assurance Quality Activity, the Document Object Model (DOM) Working Group, the Schema Working Group, the Extensible Stylesheet Language (XSL) Working Group, the Cascading Stylesheets (CSS) Working Group, the XML Working Group, and the SYMM Working Group. ITL's contributions facilitate the interoperability of the web.

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 Committee, 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. ITL promotes the security of the financial services industry through participation in this forum.

STAFF RECOGNITION

DEPARTMENT OF COMMERCE 2001 MEDAL AND NIST AWARDS

The Advanced Encryption Standard (AES) Team, consisting of (first row) Morris Dworkin, Elaine Barker, Larry Bassham, Edward Roback, (second row) James Dray, William Burr, Miles Smid, James Nechvatal, and Juan Soto (James Foti not pictured) received the Gold Medal Award for Leadership in developing the Advanced Encryption Standard. The team also received the RSA Public Policy Award for significant contributions to the application of cryptographic technologies towards the advancement of personal privacy, civil justice, and basic human rights.

Roldan Pozo and Ronald Boisvert, Mathematical and Computational Sciences Division, received the Bronze Medal Award for their leadership in technology transfer introducing significant improvements to the Java™ programming language and environment for scientific computing applications.

Michael McCabe, Information Access Division, received the 2001 NIST Edward Bennett Rosa Award for outstanding leadership in the development of law enforcement image data exchange standards.

Robert Raybold, Gale Richter, Robert Glenn, Joe Matusiewicz, and **Jeff Gift (Robert Sorensen and Sandy Yu not pictured)** received the Bronze Medal Award for their design and implementation of the NIST network firewalls in Gaithersburg and Boulder.

Joe Kau and **Audrey Houser**, Information Services and Computing Division, were part of a NIST team selected to receive a Bronze Medal Award for successfully implementing CSTARS, a new automated system to process acquisitions at NIST.

Peter Mell, Computer Security Division, received the Bronze Medal Award for conceiving, developing, and fielding the Internet Catalogue of Assailable Technologies (ICAT) vulnerability database and search engine.

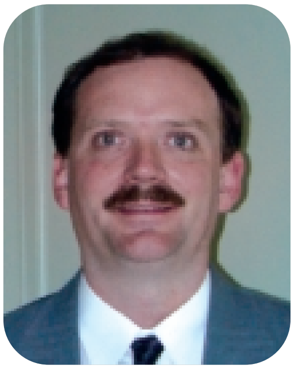
EXTERNAL STAFF RECOGNITION

Christopher Dabrowski, Software Diagnostics and Conformance Testing Division, received a 2000 Committee Management Award from the National Committee for Information Technology Standards (NCITS). The award recognizes Dabrowski's outstanding leadership, as ISO/TC 211/WG 1 Convener, in the rapid progression of the ISO 19100 series of standards for Geographic Information Systems (GIS).

Raghu Kacker, Statistical Engineering Division, was elected a Fellow of the American Society for Quality. He was honored for pioneering work in advancing the application of statistical sciences, especially Taguchi methods, to quality, measurement science, calibration, and interlaboratory comparisons.

Anthony Kearsley, Mathematical and Computational Sciences Division, was named a recipient of the prestigious Arthur S. Flemming Award for 2001, given each year to outstanding federal employees with less than 15 years of federal service. Kearsley was cited for a sustained record of contributions to the development and use of large-scale optimization techniques for the solution of partial differential equations arising in science and engineering.

Frances Nielsen and **Marianne Swanson,** Computer Security Division, received 2001 Federal 100 Awards from *Federal Computer Week* for their role in developing the Information Technology Security Assessment Framework for the Federal CIO Council. Federal 100 Awards recognize executives from government, industry, and academia who have made the greatest impact on the government systems community in 2000.



John Roberts and the E-Book/Braille Reader Development Team, Convergent Information Systems Division, received a prestigious 2001 R&D 100 Award from *R&D Magazine*. Roberts led the project team that included, over several years, Oliver Slattery, Brent Swope, Dave Kardos, Edwin Mulkens, Volker Min, Gina Rodgers, and Michael Sutton. Now in its 39th year, the international R&D 100 Awards program selects 100 of the most important, unique, and innovative technologies.

Bonita V. Saunders, Mathematical and Computational Sciences Division, presented the 2001 Claytor Lecture entitled Numerical Grid Generation and 3D Visualization of Special Functions on January 13, 2001. The National Association of Mathematicians (NAM) inaugurated the Claytor Lecture in 1980. Founded in 1969, NAM is a non-profit professional organization whose mission is "to promote excellence in the mathematical sciences and promote the mathematical development of underrepresented American minorities."

Alan Dunn, a high-school summer intern in the Computer Security Division, placed fourth in Intel's Science Talent Search. Dunn's project was to optimize the Advanced Encryption Standard finalist encryption algorithm candidates for the AltiVec vector processor of the Macintosh G4. He received a $25,000 scholarship to the college of his choice.

The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST carries out its mission through four interwoven programs:

- NIST Laboratories that provide technical leadership for vital components of the nation's technology infrastructure needed by U.S. industry to continually improve its products and services;

- a highly visible quality outreach program associated with the Baldrige National Quality Program that recognizes business performance excellence and quality achievement by U.S. manufacturers, service companies, educational organizations, and health care providers;

- the Manufacturing Extension Partnership, a nationwide network of local centers offering technical and business assistance to smaller manufacturers; and

- the Advanced Technology Program, accelerating the development of innovative technologies for broad national benefit through R&D partnerships with the private sector.

NIST has an operating budget of about $720 million and operates primarily in two locations: Gaithersburg, Maryland and Boulder, Colorado. NIST employs more than 3,200 scientists, engineers, technicians, business specialists, and administrative personnel. The website is http://www.nist.gov.

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
Web site: *http://www.itl.nist.gov*

NOTE: *Reference to specific commercial products or brands is for information purposes only; no endorsement or recommendation by the National Institute of Standards and Technology, explicit or implicit, is intended or implied.*

Sun, Sun Microsystems, the Sun Logo, Solaris, Java, and Jini are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

**Bluetooth SIG Inc. U.S.A. owns the Bluetooth trademarks.*