

ITL *TECHNICAL ACCOMPLISHMENTS*



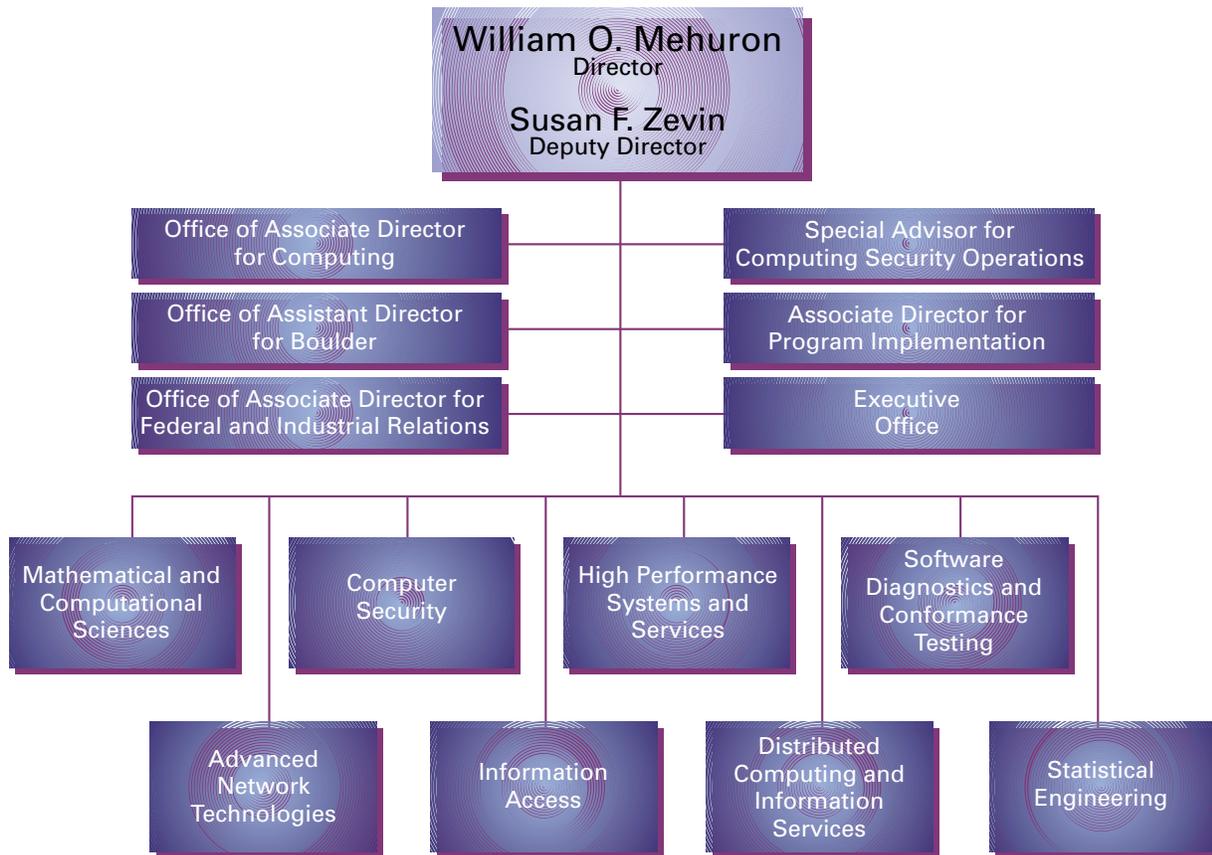
2000

NIST

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

Information Technology Laboratory
NISTIR 6558

Information Technology Laboratory



NISTIR 6558
October 2000



U.S. DEPARTMENT OF COMMERCE
Norman Y. Mineta, Secretary

Technology Administration
Dr. Cheryl L. Shavers
Under Secretary of Commerce for Technology

National Institute of
Standards and Technology
Raymond G. Kammer, Director

C O N T E N T S

Director's Foreword	1
ITL at a Glance	3
Technical Accomplishments	6
Industry Interactions	30
International Activities	37
Staff Recognition	39
Service to NIST	42

DIRECTOR'S FOREWORD

SEPTEMBER 30, 2000

The Information Technology Laboratory (ITL) is one of the Measurement and Standards Laboratories of the National Institute of Standards and Technology (NIST). Our mission is to strengthen the U.S. economy and improve the quality of life by developing and applying technology, measurements, and standards for information technology (IT). We also fulfill a legislative mandate in the computer security arena to develop standards and



guidelines for the federal government. ITL is uniquely positioned in the exploding world of information technology, providing an objective, independent, cutting-edge forum for measurements and standards development. The laboratory carries out its mission by working with industry, research, and government organizations to develop and demonstrate tests, test methods, reference data, proof-of-concept implementations, and other infrastructure technologies that are essential to the global information technology revolution. Our aim is to enable U.S. industry to produce information technology systems that are usable, secure, scalable, and interoperable.

During the past year, ITL gained significant industry and federal recognition in the four components of its role, i.e., research, measurement, standards, and service. We also participated in a variety of industry consortia and groups, influencing product development at an early stage in the evolution of particular technical fields. Examples include:

Advanced Encryption Standard (AES) - ITL completed the three-year public competition. Secretary Mineta announced the winner, Rijndael, and ITL received much positive press and recognition for the AES effort;

National Information Assurance Partnership (NIAP) - Thirteen countries signed the Mutual Recognition Agreement. ITL co-sponsored the first international conference on Common Criteria (CC). The first four

laboratories were accredited, and the final smart card security specifications were published in a CC Protection Profile;

Extensible Markup Language (XML) - ITL chaired the XML standards committee on behalf of the Organization for the Advancement of Structured Information Standards (OASIS), led the technical development of the XML conformance test effort and developed many of the tests, and coordinated the effort that resulted in contributions from individual member companies. ITL is developing a reference implementation for the registry/repository of XML vocabularies for use in vertical markets;

Digital and Interactive TV - ITL chairs the Digital TV Application Software Environment (DASE) conformance working group with major television networks and computer providers, and partners with industry to develop conformance tests and a reference implementation for the programming environment. ITL developed a prototype receiver testbed and a standard for Internet content and bindings to analog and digital streams;

Pervasive Computing - ITL built a unique microphone array for meeting room speech acquisition and processing, and delivered a sensor array and data flow systems to four collaborating laboratories;

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. The work appears on the cover of *Physics Today* (December 1999);

Braille Reader - ITL scientists developed, demonstrated, and patented two prototypical Braille readers, a technology which could enhance accessibility to the Internet and electronic media for the visually challenged;

Biometrics and Smart Cards - ITL demonstrated the interoperability of biometric subsystems and integrated these into smart cards, developed the biometric applications programming interface, and helped forge the industry alliance known as the Biometric Consortium; and

Digital Library of Mathematical Functions - In this multi-year project, ITL is fundamentally changing access to standard mathematical functions reference data by creating an online, interactive digital mathematical library. This year all chapter outlines were completed, and contracts with contributing authors have been let.

We continued our work on the largest of our new initiatives. This is the laboratory-wide pervasive computing focus in which ITL continues its leadership role in 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.

An extension of this work will be the development of technologies to ensure IT access for people with disabilities. Another ITL initiative involves working with industry to develop benchmark tests for evaluating Web usability. In new, groundbreaking work, ITL mathematicians, cryptographers, telecommunications specialists, and software experts are working with NIST physicists on theories to develop quantum computation and quantum information systems.

In addition to interactions with industry communities, we continue to have a positive impact on other laboratories within NIST by providing research collaborations and technical services. The Mathematical and Computational Sciences Division and the Statistical Engineering Division support work in other NIST laboratories and perform crucial services in areas such as modeling and validation of standards activities. Further, ITL provides vital services to the entire NIST community. These services include networking, high performance computing, computer support for desktop 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 provide the technical leadership for the Nation's measurement and standards infrastructure for information technology, as well as needed information technology products and services to promote the U.S. economy in the global marketplace.

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*

Fred Johnson, *Associate Director for Computing*

Paul Domich, *Assistant Director for Boulder*

Barbara Guttman, *Associate Director for Federal and Industrial Relations*

Robert Glenn, *Special Advisor for Computing Security Operations*

Associate Director for Program Implementation (vacant)

Kendra Cole, *Senior Management Advisor*

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

Kevin Mills, *Chief of Advanced Network Technologies Division*

Edward Roback, *Acting Chief of Computer Security Division*

Martin Herman, *Chief of Information Access Division*

Victor McCrary, *Acting Chief of High Performance Systems and Services Division*

Dale Spangenberg, *Chief of Distributed Computing and Information Services Division*

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

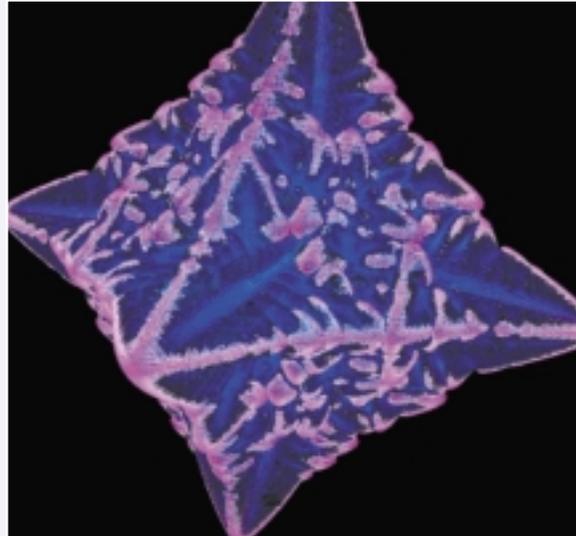
Nell Sedransk, *Chief of Statistical Engineering Division*

ITL Mission

Our goals are to strengthen the U.S. economy and improve the quality of life by providing the information technology industry and users with needed measurements and standards 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



A simulated dendrite of a copper-nickel alloy as it is growing with surface coloring to represent the relative concentration of the two metals. The simulation is implemented as a parallel program using MPI (Message Passing Interface) and high performance visualization in a collaboration between James Warren of the NIST Material Science and Engineering Laboratory and ITL (William George and Steve Satterfield).

ITL Products and Services

- reference data sets and evaluation software
- proof-of-concept implementations
- 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 460 (includes part-time), supplemented by 118 guest researchers and faculty members (as of September 23, 2000)
- total fiscal year 2000 budget of \$76.8M, all sources
- state-of-the-art research facilities in Gaithersburg, Maryland, and Boulder, Colorado
- opportunities for cooperative research and interaction with industry and academia

ITL Technical Divisions

● The **Mathematical and Computational Sciences**

Division provides technical leadership within NIST in modern analytical and computational methods for solving scientific problems of interest to industry. The division focuses on the design of experiments, modeling, analytical methods, and algorithms for science.

● The **Advanced Network Technologies Division** works with the networking industry to improve the quality of technical standards, and to raise the robustness, scalability, and performance of products implemented to meet those standards. The division brings to this task expertise in formal modeling and analysis of specifications; in modeling, analysis, and measurement of protocol performance; and in testing of protocol implementations for conformance to specifications and for interoperability with other implementations.

● The **Computer Security Division** raises awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies; researches, studies, and advises agencies of IT vulnerabilities and devises techniques for the cost-effective security and privacy of sensitive federal systems; develops standards, metrics, tests and validation programs; and develops guidance to increase secure IT planning, implementation, management, and operation.

● The **Information Access Division** accelerates the development of technologies that allow intuitive, efficient access, manipulation, and exchange of complex information by facilitating the creation of measurement methods and standards. These technologies include user interfaces, text retrieval, speech and human identification, and computing study and measurement.

● The **High Performance Systems and Services Division** enables the effective application of high performance computing

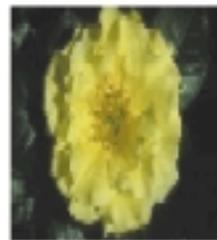
Query by example (image 1) by an algorithm developed at NIST



1



2



3



4



5



6



7



8



9



10



11



12

and communications systems in support of the U.S. information technology industry. The division conducts research, development, and evaluation of convergent technologies, disciplines, and information services leading to innovative measurement and test methods for improved computing performance, scalability, functionality, interoperability, flexibility, reliability, and economy.

● The **Distributed Computing and Information Services Division** provides the information technology resources, supporting infrastructure, applied research, and assistance to NIST staff, collaborators, and clients for application in the conduct of scientific, engineering and administrative applications and in the dissemination of information.

● The **Software Diagnostics and Conformance Testing Division** develops software testing tools and methods that improve quality, conformance to standards, and correctness. The division also participates with industry in the development

of forward-looking standards and leads efforts for conformance testing, even at the early development stage of standards.

● The **Statistical Engineering Division** catalyzes scientific and industrial research through the application of statistical methods to experimentation and data analysis. Division statisticians provide expertise to NIST scientists and collaborative partners in industry in the development of modeling techniques and analysis relevant to measurement science and technology.

Descriptions of selected ITL technical accomplishments for FY 2000 appear in the following section.

Querying by example (same image) in a commercial scheme based on color-distribution



1



2



3



4



5



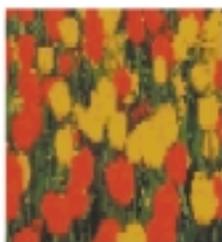
6



7



8



9



10



11



12

Mathematical and Computational Sciences Division Projects

Digital Library of Mathematical Functions (DLMF)

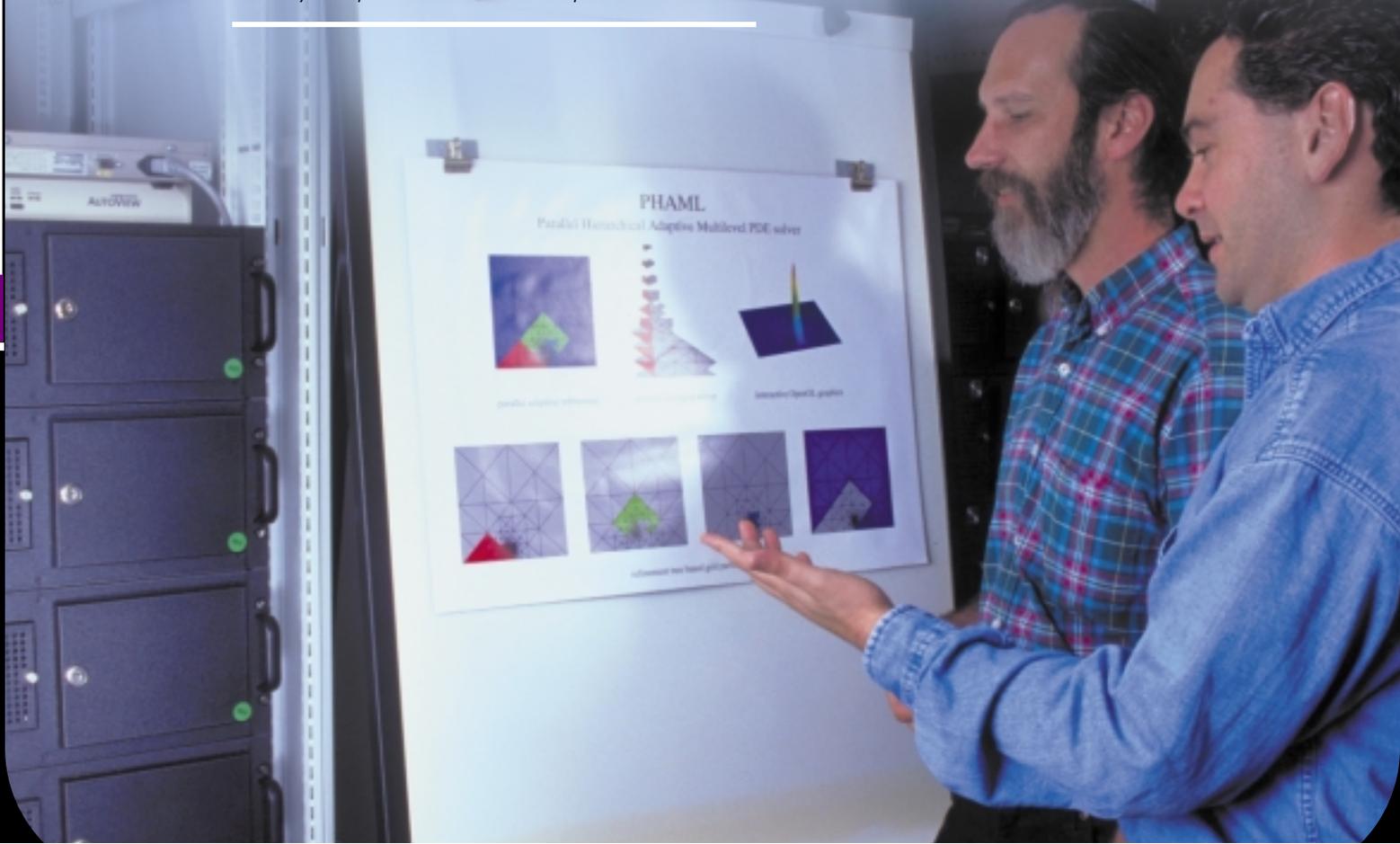
ITL continues to develop and enhance its Digital Library of Mathematical Functions, an interactive, richly linked, network-based resource of mathematical reference data from a variety of fields. Freely accessible on the Web, the DLMF will provide some of the basic infrastructure needed by the technical community to integrate modern information technology more fully into its day-to-day work. The digital library will replace the classic *Handbook of Mathematical Functions*, Applied Mathematics Series 55, published by our agency in 1964. This important reference contains formulas, graphs, and tables, which characterize the higher functions of applied mathematics. These functions (often known as special functions) are used extensively in mathematical analysis in many fields, such as physics and chemistry, and they are essential tools in modern computational model-

ing of phenomena in the physical sciences and engineering. In FY 2000, ITL hosted the second editorial board meeting, identified the remaining authors and contracted for chapter outlines, and completed guidelines for authors and validators. We also developed the DLMF LATEX style computer files and distributed the DLMF LATEX style guide. Finally, we provided a password-protected Web site for project participants, contracted with some authors for full chapters, and provided VRML graphics improvements and applications to more functions. The Web site is <http://math.nist.gov/DigitalMathLib/>.

Fortran 90 Bindings for OpenGL®

As part of this ITL project initiated in 1996, researchers specified complete Fortran 90 bindings for OpenGL® and developed a portable reference implementation for the bindings. We continue

W. Mitchell describes to A. Kearsley the powerful grid partitioning methods that he developed to support parallel multigrid solution of boundary value problems on PC cluster computers.



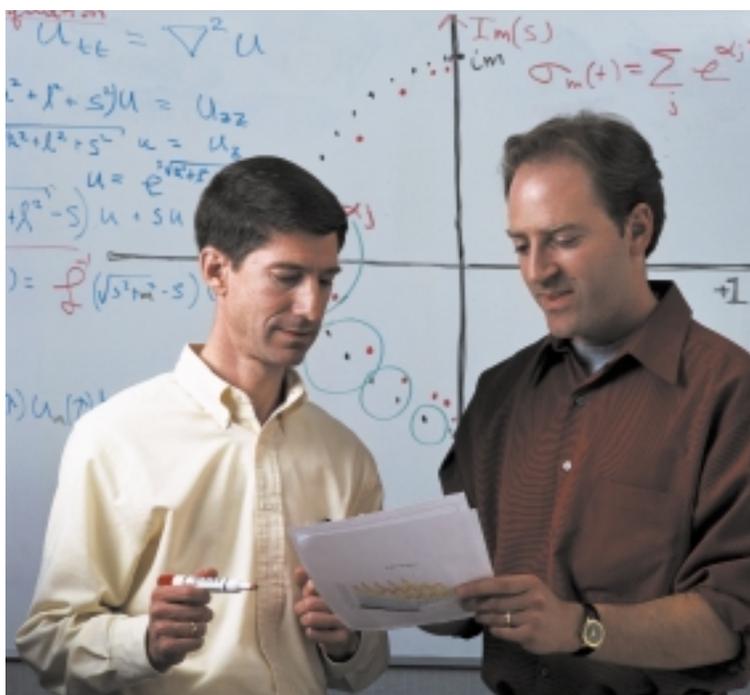
to work with external groups to have the bindings adopted as industry standards. The Fortran 2000 standard will contain facilities for C interoperability. In FY 2000, we completed the preliminary design of f90gl using the C interoperability standard and released f90gl Version 1.2.2. Our work brought out several deficiencies in the proposed interoperability standard, not just for f90gl, but also for interfacing with other C programs and libraries. We met with J3, the U.S. Fortran Standards Committee, to discuss these deficiencies and proposed several changes to the draft standard, most of which were accepted. The Web site is <http://math.nist.gov/f90gl/>.

Guide to Available Mathematical Software (GAMS)

GAMS is an online service that provides access to information about mathematical and statistical software of use in computational science. It provides information about software available to NIST staff on its internal systems as well as information about software available from netlib, the premier repository for software developed by the numerical analysis research community. (netlib is operated by ORNL, the University of Tennessee and Bell Labs.) GAMS provides information about some 8,800 software components from 108 packages, both proprietary and public domain. In FY 2000, we continued to revise and update the GAMS server and database to keep current with software assets available on NIST systems as well as software available from netlib. The Web site is at <http://math.nist.gov/gams/>.

Java™ Numerics

ITL continues to support community efforts to improve the Java™ language and environment for high-performance scientific computing. Through our participation in the Java™ Grande Forum, we conduct assessments of the potential of Java™ for scientific computations, hold public meetings to discuss issues and provide input to Sun Microsystems, and develop community-supported standardized class libraries for core mathematical computation. Two ITL staff members co-chair the Numerics Working Group of the Java™ Grande Forum. In FY 2000, we organized a panel at the SC 99 conference on Java™ Grande activities and facilitated Sun's adoption of the Numerics Working Group elementary function proposal Java™ Spec Requests (JSRs) for fastfp and Array API. We hosted a group meeting at the ACM Java™ Grande Conference, organized a mini-symposium on Java™ at the SIAM National Meeting, and participated in the Dagstuhl seminar on Java™. Finally, we completed the draft JSRs for complex numbers and complex class and initiated the Java™ Community Process work for fastfp and Array class. The Web site is <http://math.nist.gov/javanumerics/>.



B. Alpert describes his work on electromagnetic modeling to A. Dienstfrey. Alpert has developed new techniques for the rapid evaluation of nonreflecting boundary kernels for time-domain wave propagation.

Measurement Science for Optical Reflectance and Scattering

The objectives of this NIST competency project are to explore the relationship between material microstructure of a surface and its appearance, determine the feasibility of rendering as a tool for simulating surface appearance from measurements, and create a NIST-based measurement database to be used by the computer graphics, paint, automotive, and other industries concerned with the appearance of coated surfaces. The competency project group sponsored a workshop at NIST on March 29-30, 2000. The meeting brought together industrial researchers who must use appearance measurements in product development and computer scientists doing research on computer rendering and related computer graphic techniques. The workshop purpose was to discuss technical advances in appearance measurement research and to provide a forum for a discussion of industrial appearance issues that NIST and the industries could address. This year, we also completed our research on software for the measurement database.

The Web site for rendered data is <http://math.nist.gov/mcsd/Staff/FHunt/webpar4.html>.

Micromagnetic Modeling

Advances in magnetic devices such as recording heads, field sensors, and magnetic nonvolatile memory are dependent on micro-structural details for their high performance. Accurate micromagnetic modeling is critical for design and development of such devices. ITL is collaborating with NIST's Materials Science and Engineering Laboratory to develop reference, open-source micromagnetic modeling tools, with experimental verification. In April 2000, we officially released the micromagnetic package, OOMMF v1.1, followed by the alpha release in August of the micromagnetic package with 3D solver. We also sponsored an OOMMF Workshop at NIST in August 2000. Industry partners in the project include IBM, Quantum, the University of New Orleans, the University of Alabama, and the University of Maryland. Several companies in the computer hard drive industry are using the code. The Web site is <http://math.nist.gov/oommf/>.

OOF: Object Oriented Finite Element Software for Materials Science

ITL and NIST's Materials Science and Engineering Laboratory are developing software that can read a micrograph, assign microscopic materials properties to features in the image, perform virtual experiments to determine the macroscopic properties of the material, and extract useful results. The software should be usable by researchers with no experience in programming or finite element methods. In addition, the software should be easily modifiable to handle new types of materials. Since the release in FY 1996 of the first working versions of PPM2OOF (for assigning

properties to images) and OOF (for performing virtual experiments), numerous enhancements and features have been added. In FY 2000, we began work on version 2, to include new physical phenomena such as piezoelectricity and thermal diffusion. We also changed the underlying user interface routines to allow more flexible scripting and (possible) port to non-Unix architectures. The Web site is <http://www.ctcms.nist.gov/oof/>.

The NIST Sparse BLAS

In cooperation with the BLAS Technical Forum, ITL is developing community standards for sparse matrix kernels. This work includes the development of interface specifications, reference implementations, and a project Web site. External participants in the effort include SGI/Cray Research, Sandia National Laboratory, Rutherford Appleton Laboratories (UK), the University of Minnesota, the University of Tennessee at Knoxville and The BLAS Technical Forum, an industry/government/academic working group with participants from SGI/Cray, NEC, Intel, the Numerical Algorithms Group, Ltd., Lucent Technologies, HP/Convex, Tera Computers, Texas Instruments, Visual Numerics, and IBM. This year, we released a draft version of the reference implementation (software) for public review, followed by the release of the final version in the public domain in the fourth quarter of FY 2000. The Web site is <http://math.nist.gov/spblas/>.

Time-Domain Algorithms for Computational Electromagnetics (AlgoCEM)

Radiation and scattering of acoustic and electromagnetic waves are increasingly modeled using time-domain computational methods, due to their flexibility in handling wide-band signals, material inhomogeneities, and non-linearities. For many applications, particularly those arising at NIST, the accuracy of the computed models is centrally important. ITL is advancing the state of the art in electromagnetic computations by eliminating three existing weaknesses with time-domain algorithms for computational electromagnetics through the development of software to verify the accuracy of the new algorithms. In FY 2000, we conducted numerical experiments for spherical harmonics transform and performed further numerical experiments on new formula for discretization (two dimensions). We discovered a new technique for model reduction arising out of work on nonreflecting boundary conditions. In conjunction with further numerical experiments, we began the implementation of fast spherical harmonics transform. The Web site is <http://math.nist.gov/mcsd/>.



The Digital Library of Mathematical Functions team: standing, from left to right, M. McClain, B. Fabijonas, C. Clark (Physics Lab), R. Boisvert, and B. Miller; seated, from left to right, B. Saunders, F. Olver, and D. Lozier. Not pictured: J. Conlon and Q. Wang (Information Access Division).

Advanced Network Technologies

Division Projects

All-Optical Transport Networks with Wave Division Multiplexing (WDM)

To meet the goals of the Next Generation Internet (NGI) Presidential Initiative, next-generation networks must be ultra-fast, scalable, and rich in services. ITL focuses on the metrology for dense WDM, evaluation network control mechanisms, and support of Internet Quality of Service (QoS) and Traffic Engineering. We collaborate in this work with designers and vendors of WDM component simulation software, including Telcordia, BNed, and ARTIS. We also work with members of standards groups and industry consortia such as the ANSI Committee T1 and the Optical Internetworking Forum. In FY 2000, we evaluated signaling

protocols for Internet Multi-Protocol Label Switching (MPLS) over WDM networks and reported our findings. We also released MERLiN, Version 1.0, a tool for network planning and research in wavelength routing, assignment, and reconfiguration. The Web site is http://w3.antd.nist.gov/Hsntg/prd_merlin.html.

Characterization of Broadband Wireless Communication Systems

To provide cable TV, telephone, facsimile, Internet access, and other data services to business and residential users through a single, unified broadband access mechanism, ITL researchers are working with a system called Local Multipoint Distribution Service (LMDS).

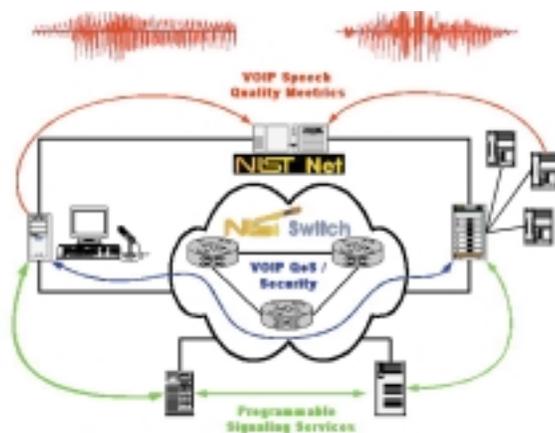
H. Gharavi discusses his work on a dual-priority transmission scheme for sending H.263 video over the W-CDMA third-generation wireless system with N. Moayeri.



LMDS can be a viable alternative to competing technologies such as cable-modem and DSL in areas where in-ground cabling is not available. Working closely with NIST's Electronics and Electrical Engineering Laboratory, we developed several channel propagation models for LMDS to capture effects of precipitation, blockage by tree foliage, LOS vs. non-LOS channel conditions, diffraction, and other factors. Industry will benefit from this work if LMDS can achieve excellent communication quality at a lower cost than competing technologies.

Future Generation Wireless Communication Systems

ITL is developing software simulation models for various technologies proposed for future generation wireless communication systems, evaluating the performance of these technologies, and developing new, improved methodologies. Other project goals include the development of new techniques for transport of multimedia data over mobile wireless channels and contributions to the development of national and international standards for future generation wireless communication systems. In FY 2000, working with Cadence Design Systems, Inc., we completed the



validation of SPW models developed for the cdma2000 system, including the forward / reverse links, the fundamental / supplemental / paging / sync / pilot channels, and released the new models. We also evaluated the performance of the cdma2000 system for various traffic patterns and under various communication channel conditions corresponding to mobile vs. stationary users, different geographic terrain, and wireless user density. Wireless operators, equipment manufacturers, and application developers will benefit from this work, especially smaller companies with limited resources.

Internet Security and IPv6 Technologies

This ITL project seeks to expedite the research, development, standardization, and commercialization of next-generation Internet security and IPv6 technology. Our Computer Security Division collaborates in this work. In FY 2000, we focused on the integration of security systems, in particular the incorporation of advanced authentication mechanisms and PKIX in IPsec and IKE. We analyzed multicast key distribution algorithms and schemes. We released Cerberus 0.5, which supports an advanced encryption standard (AES) and enhanced policy management, and Cerberus V6, the prototype of Cerberus for IPv6. IPsec-WIT was updated to support testing with digital signatures and AES algorithms. We also initiated research on the Integrated Security Systems Simulator for large-scale analysis of IPsec systems performance. Finally, we looked at technology for Internet infrastructure protection, specifically the development of test and measurement tools for DNSSec. The Web site is http://w3.antd.nist.gov/Projects/projects_antd.html.

IP Quality of Service

ITL actively participates in the design, standardization, development, and testing of next-generation internetworking technology. These activities focus on current design and standardization efforts within the Internet Engineering Task Force (IETF) to add significant new functionality to the Internet Protocol Suite (IPS). One such area is the transmission of real-time, Quality of Service (QoS) sensitive traffic over Internet technologies. In FY 2000, we designed and analyzed routing algorithms to support QoS and traffic engineering in Multi-Protocol Label Switching (MPLS) networks. We also experimented with integrated routing, label distribution, and signaling protocols to support traffic engineering in MPLS networks. Finally, we designed and analyzed MPLS-based mechanisms to support dynamic virtual overlay networks (VONs). ITL's IP QoS testing tools are used extensively by the IETF/Internet research and development community. The Web site is http://w3.antd.nist.gov/Projects/projects_antd.html#Internetworking.

Mobile Ad Hoc Networks

The next generation of wireless communication systems will require the rapid deployment of independent mobile users. In response to this need, ITL facilitates the development of protocols and standards for MANETs, which are autonomous collections of

mobile users (nodes) that communicate over wireless links. In FY 2000, SAIC installed the Defense Advanced Research Projects Agency (DARPA)-developed SEAMLSS wireless network simulation and testing tool at NIST. We tested and verified different versions of the SEAMLSS environment. We verified DARPA GloMo SEAMLSS environment, version 1.6, and DARPA GloMo SEAMLSS environment, version 2.0. We also investigated the usefulness of MANETs for NS/EP applications. Collaborators in this project include SAIC, DARPA, NCS, CECOM, IETF, and respective proposers of MANET protocols from academia and industry. The Web site is <http://w3.antd.nist.gov/wctg/index.html>.



W. Chang hosts the NIST MPEG-4 repository Web site for bit-streams interoperability testing between vendors and makes the reference implementation of MPEG-4 players software available within the MPEG-4 community.

MPEG and Image Compression Tools

ITL facilitated the development of multimedia applications and standards (MPEG-2 extensions, MPEG-4, MPEG-7, SMIL, and multimedia indexing) by developing tools, image fidelity metrics, and standard reference materials. Through contributions and maintenance of Web facilities, we supported the work of the MPEG committees. In FY 2000, we conducted research in image indexing and video restoration, developing image indexing schemes, images, and video clips to demonstrate the limitations of pixel and frame-based metrics. Our performance evaluations show that our techniques are superior to existing ones in terms of retrieval outcomes. We expedited the development and testing of SMIL, a W3C standard. The project concluded at the end of the fiscal year.

Networking for Pervasive Computing

ITL validates the protocols that will enable wireless devices to operate in a pervasive computing environment and evaluates the performance of these technologies for coexistence. We also assess the state of dynamic discovery technology in industry and academe, to propose metrics to evaluate dynamic discovery technology and to evaluate some of the leading technical standards. In FY 2000, we modeled the Link Manager Protocol (LMP), Logical Link Control Adaptation Protocol (L2CAP), and Baseband (BB) protocol in Specification and Description Language and submitted to IEEE 802.15.1 for inclusion into the draft standard. ITL serves as the co-chair of the Task Group on Coexistence, IEEE 802.15.2. We developed Models for Bluetooth™ Protocol MAC Specifications using the Opnet tool. We developed a prototype wireless Jini™ adapter and made performance measurements of the adapter. Finally, we updated the models of LMP, L2CAP, and Baseband in line with revisions to the Bluetooth Specification and the draft IEEE 802.15.1 standard and integrated the three models into a single device model.

Programmable Network Technology

ITL pursues the research and development of advanced, programmable network technologies. Specific goals include the research and development of adaptive middleware to enable scripting of configurable distributed systems and the development of test and measurement techniques to enable resource control in active networks. In FY 2000, we completed our research and development of reliable peer-to-multi-peer protocols that support dynamic reconfiguration and mobility. We developed a simulation toolkit for reconfigurable distributed systems and analyzed algorithms for adaptive, reconfigurable control mechanisms. We also released the final version of AGNI, a distributed systems framework and toolkit based upon an abstraction called Mobile Streams. We proposed a standard metric for measuring computational resources among heterogeneous nodes in an active network. This work includes defining a meaningful metric for processing requirements and creating the needed tools to effectively use that metric in an active network.

Computer Security Guidance

As specified in OMB Circular A-130, NIST advises federal civilian agencies on computer security issues. In FY 2000, we issued ITL Bulletins and Special Publications on intrusion detection systems, operating system security, security implications of active content, analysis of hacking trends, and mobile agent security. Publications in progress address PBX security, firewall policy, incident-handling guidance, and PKI essentials. We initiated a new series of publication, NIST Recommendations, the first being a *Guideline to Federal Organizations on Assessing Information Technology (IT) Security Programs*. The Web site is <http://csrc.nist.gov>.

Computer Security Resource Center (CSRC)

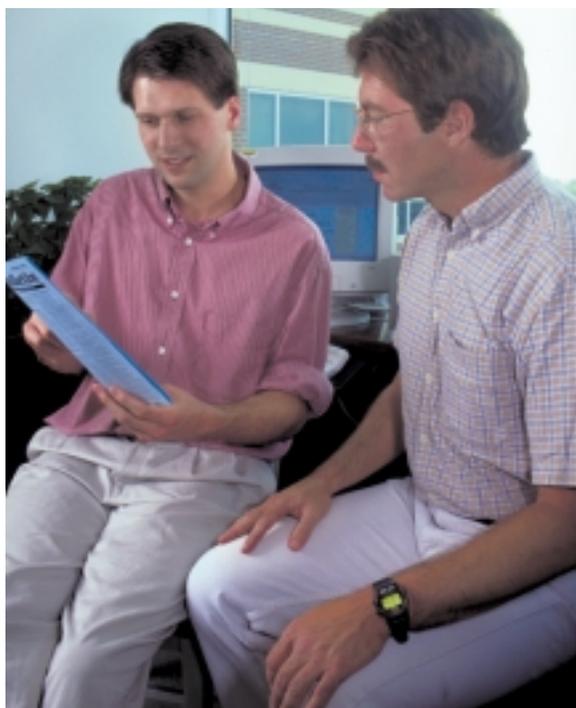
The CSRC represents NIST's work in developing, prototyping, testing, and implementing computer security standards and procedures to increase security measures and to create more robust security architectures. In FY 2000, we redesigned the CSRC. We coordinated the site content with the CIO Council Security Committee, added large sections on training and the ICAT project, and improved searching and navigating features such as a site map/index and searching capability from all pages. Finally, we added accessibility features to the Web pages to improve usability for sight-impaired users. The Web site is <http://csrc.nist.gov>.

Cryptographic Module Validation Program (CMVP)

The CMVP provides a documented methodology for conformance testing through a defined set of security requirements in FIPS 140-1, *Security Requirements for Cryptographic Modules*, and other cryptography-based standards. The results of the independent testing performed by one of four accredited laboratories provide a security metric to use in procuring equipment containing cryptographic modules. In FY 2000, we achieved our 100th validation certificate. In addition, we updated FIPS 140-1 and will publish it as FIPS 140-2 in FY 2001. The Web site is <http://csrc.nist.gov/cryptval>.

Cryptographic Toolkit Standards

Initiated in FY 2000, this ITL project seeks to complete and upgrade the cryptographic algorithm standards to be used by the federal government for the protection of sensitive but unclassified data. The standards specifying these algorithms must be testable by the FIPS 140-1 CMVP. In April, we sponsored a Key Management Standard Workshop. Other workshops, testing, and standards-development work are planned over the next four years. The development of the cryptographic tool kit is a multi-year effort.



P. Mell and J. Wack discuss anti-hacking guidance.

Encryption Key Recovery

ITL continued to support the industry advisory committee on encryption key recovery within the federal government. The goals of the project are to ensure private sector involvement in the development of key management infrastructure requirements and to obtain technical recommendations of the advisory committee for the development of appropriate federal standards. In FY 2000, NIST evaluated public comments received on the committee's report and made recommendations on the future development of a federal standard for encryption key recovery. The Web site is <http://csrc.nist.gov/tacdfipsfkmi/>.

ICAT Metabase

In FY 2000, ITL designed and developed the ICAT Metabase. This searchable index of computer vulnerabilities links users into a variety of publicly available vulnerability databases and patch sites, thus enabling one to find and fix the vulnerabilities existing on their systems. In March, we created the prototype ICAT metabase. In May, ICAT became a Web-based application, and in July, ICAT caught up with the Common Vulnerabilities and Exposures (CVE) vulnerability-naming standard by categorizing 700 vulnerabilities. The Web site is <http://csrc.nist.gov/icat>.



S. Chang and D. Cooper are working to resolve PKI implementation interoperability issues.

IT Security Training and Awareness Resource Center

Funded by the Government Information Technology Services (GITS) Board, this project established a single focal point for IT security training in the federal government. NIST developed the database keyed to the training needs identified in NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, which provided the taxonomy against which the training materials were cataloged. The Web site allows for access by user role, information content, and technology type, as well as type of training media. The Web site is <http://patapsco.nist.gov/itl/div893/gits/main.html>.

Mobile Agent Intrusion Detection and Security Research

ITL researchers are evaluating the use of mobile agents for performing network security testing. Funded by NSA, our research focuses on restricting mobile agents' capabilities on a host using digitally signed passports and using mobile agent technology to enhance intrusion detection systems. In addition to our cooperative research agreement with Boeing, we are working with a number of other mobile agent research groups to build a secure mobile agent architecture. In FY 2000, we published NISTIR 6416, *Applying Mobile Agents to Intrusion Detection and Response*, available at <http://csrc.nist.gov/publications/nistir/index.html>.

National Information Assurance Partnership (NIAP)

A collaboration between NIST and NSA, NIAP is the federal initiative to meet the security testing needs of both IT consumers and

producers. In FY 2000, NIAP developed an automated Toolbox for construction of Common Criteria (CC)-based protection profiles and security targets. NIAP also sponsored the First International Common Criteria Conference. In addition, four private sector security testing laboratories were accredited and operation of the Common Criteria Evaluation and Validation Scheme commenced. The Web site is <http://niap.nist.gov/>.

Public Key Infrastructure (PKI)

ITL is working with industry to develop a set of security requirements and tests for PKI components. In FY 2000, we specified and published security requirements for a Common Criteria Protection Profile (PP) for Certificate Issuing and Management Components (CIMC). We also published the Minimum Interoperability Specification of PKI Components (MISPC) V2. In addition, we developed a PKI interoperability testbed, including Secure/Multipurpose Internet Mail Extensions (S/MIME) interoperability testing, and an MISPC reference implementation. The Web site is <http://csrc.nist.gov/pki/>.

Random Number Generation and Testing

In collaboration with the Statistical Engineering Laboratory, division researchers developed a set of statistical tests that may be used to verify that the output of a cryptographic random number generator (RNG) appears to match the Bernoulli (fair coin toss) model. We applied these tests to the NIST FIPS-approved random number generators and to several cryptographic algorithms. In FY 2000, we defined, programmed, and published the test set. The financial and cryptographic product communities benefit from this work. The Web site is <http://csrc.nist.gov/rng>.

S/MIME and Key Recovery Demonstration Project

ITL continued to support the development of secure and interoperable S/MIME products and the deployment of large PKIs using the bridge Certification Authority (CA) concept. ITL developed much of the basic theory of bridge CAs and provided technical support for the establishment of a Federal Bridge CA (FBCA) by the Federal PKI Steering Committee for the federal government's PKI. In FY 2000, we participated in FBCA demonstrations and testing. We also developed a S/MIME V3 feature set and test scenarios and distributed the draft S/MIME V3 profile identifying interoperability and security requirements for federal agency use. The Web site is <http://csrc.nist.gov/krdp/>.

Information Access Division Projects

Digital Video Test Collection

To address the scarcity of reusable public domain digital video data, ITL is building a public domain digital video test collection with support from an Advanced Technology Program intramural grant. The goals of the project are to create a test collection of digital video for use by researchers, to promote its use, and to gather feedback to guide its improvement. In FY 2000, we created the initial test collection and built a Web site as a mechanism for information and feedback. We produced and released Standard Reference Data: DVD, Volume I. We established a steering committee consisting of several TREC veterans and other industry and academic researchers. Finally, we drafted a Video Retrieval Track proposal for the next Text REtrieval Conference (TREC). The Web site is <http://www.itl.nist.gov/iad/894.02/projects/dv/>.

Fingerprint / Law Enforcement Standards

ITL provides the FBI with the research and development efforts required for the creation of standards, specifications, and evaluations relating to the quality, format, and transmission of electronic images and related data over a wide-area network. NIST's authority as a registered and certified ANSI standards developer is exercised to coordinate the development of official ANSI data and image interoperability standards. These efforts support the FBI's Integrated Automated Fingerprint Identification System (IAFIS) for the paperless submission, processing, and interchange of electronic fingerprint and mugshot images and data. In FY 2000, we

J. Cugini, S. Laskowski, and P. Hsiao exploit advanced visualization techniques to understand how users behave within a Website. These studies support improved Website usability.





A. Godil manipulates a lego robotic vehicle for a collaborative engineering testbed environment integrated with a Virtual Reality environment

published ANSI/NIST-ITL 1-2000, *Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information*. We also released *Special Database 27: Fingerprint Minutiae from Latent and Matching Tenprint Images*. The Web site is <http://www.nist.gov/itl/div894/894.03/fing/>.

Human ID

Formerly known as face recognition, this ITL project seeks to provide databases and human recognition performance measurement metrics and the software tools appropriate to each, to the human identification community. NIST's Office of Law Enforcement Standards collaborates in this work. The objective is to allow users to conduct their own tests and evaluations autonomously. The project involves three phases: collection of imagery, database construction and maintenance, and scoring software. In FY 2000, we initiated the collection of data for the Human ID database and released, in the fourth quarter of the fiscal year, the first installment of the database. In addition, ITL plans to release its own face recognition system; the software is an implementation of previously published image processing and recognition algorithms integrated to provide an efficient "baseline" performance frontier with which other possibly proprietary technologies can be compared. Development of this engine is ongoing.

NIST Smart Space Testbed

The NIST Smart Space Testbed began in early 1999 in response to the needs of industry and government programs aimed at develop-

ment of a new generation of computing capabilities. These are based on perceptual interfaces, pervasive (or ubiquitous) devices, agile networking, and large-scale information retrieval brought together to facilitate individual and collaborative Smart Work Spaces, such as command centers, medical examination rooms, intelligent conference rooms, or distance learning facilities. ITL is creating a modular testbed that supports integration and distributed processing of and for various sensors and classification components supported by industry. We also develop metrics and measurement techniques for recognition and signal acquisition technologies under development by industry. In FY 2000, we created the initial internal version of the NIST Smart Flow Modular Testbed. We presented the project at the NIST Pervasive Computing 2000 Conference. We conducted an initial joint data-gathering project with industrial advisors. We completed the initial test deployment of the NIST Smart Flow Modular Testbed to industrial customers. We conducted a pilot data set acquisition with the Human ID program resulting in 80 gigabytes of speech data. Finally, we launched the NIST Smart Space Web site at <http://www.nist.gov/smartspace/>.

Spoken Language Technologies Benchmark Tests, Corpora, and Software Tools

ITL develops test protocols, speech corpora, and software tools for the evaluation of spoken language technologies and has implemented benchmark tests of these technologies and reported results at Department of Defense workshops since 1987. Our researchers facilitate the development of spoken language technologies by developing test protocols and speech corpora for the training, development, and evaluation of these technologies. To date, ITL has produced over 250 speech corpus CD-ROMs. Over time, as spoken language technologies have improved, we increased the difficulty of the benchmark tests and re-targeted the test domains to continue to advance the state of the art. For instance, as Continuous Speech Recognition technology improved, ITL moved the benchmark tests from contrived, constrained domains to real-world challenges posed by radio and television news broadcasts in several languages. In FY 2000, we conducted comprehensive broadcast news tests. The Web site is <http://www.nist.gov/speech/>.

Text REtrieval Conference (TREC)

While maintaining a focus on core retrieval technology, ITL's TREC annual conference series expanded to include evaluations of different related technologies. Co-sponsored by the Defense Advanced Research Projects Agency and other Department of Defense organizations, eight conferences have been held to date. The particular technologies tested in a given year depend on the interests of the community, the needs of the sponsors, and the suitability of the problem to the TREC environment. Recent TRECs have evaluated document filtering, retrieval of speech, and retrieval of Web pages. An initial evaluation of question answering systems was introduced in TREC-8, held in November 1999, in which 66 groups participated. In FY 2000, we developed metrics for assessing search results in multi-lingual environments including non-European languages (e.g., Mandarin, Hindi). We also designed and implemented initial test scenarios for assessing search results in multimedia using videos. The Web site is <http://trec.nist.gov>.

Usability Engineering and WebMetrics

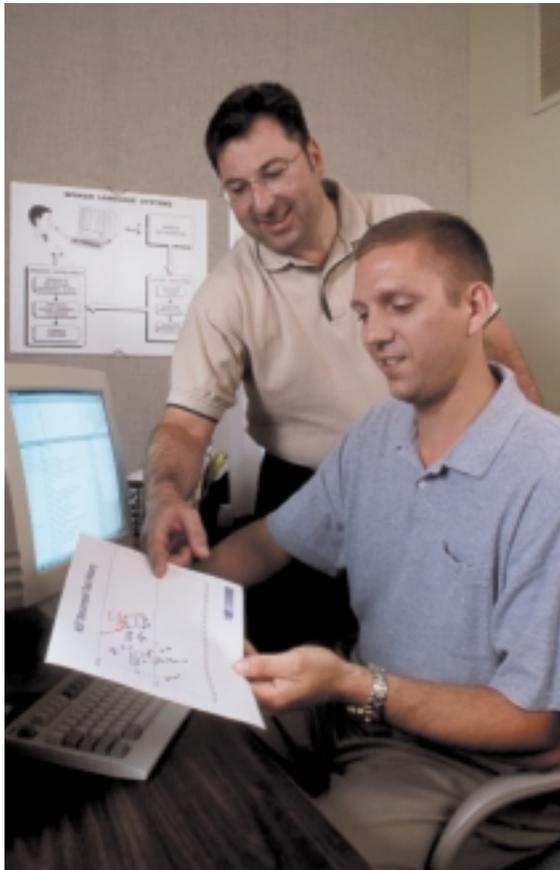
The usability engineering effort in ITL began with a series of symposia for federal government personnel, but grew into a research project aimed at improving the usability of Web sites through research in this arena and the development of tools based on the research to improve usability. We are also spearheading an industry effort to develop methods for incorporating usability into procurement decisions in the form of an ongoing series of workshops. In FY 2000, we further developed usability tools to support IEEE Web standards, accessibility, and next-generation WebMetrics tools. We advanced the effort to standardize the Common Industry Format (CIF) for usability reporting by finalizing the CIF v1.1, appendices, and template. We initiated the CIFter project to establish a benchmark for Web site evaluation. We also developed a Java™ version of the WANDS (Wide Area Network Delay Simulation) tool. Finally, we sponsored the Third Industry Usability Workshop. The Web sites are <http://www.nist.gov/webmetrics>, <http://www.nist.gov/iusr>, and <http://www.nist.gov/cifter>.

Visualization and Virtual Reality for Manufacturing

Collaborating with NIST's Manufacturing Engineering Laboratory, ITL investigates the use of advanced visualization environments to enable more intuitive interfaces to manufacturing data. Currently

in its sixth year, the project has achieved many of its objectives. We created a number of prototype systems, primarily in the Virtual Reality Modeling Language (VRML), that were the first of their kind and proved the feasibility of VRML in this domain. We are now exploring the use of tangible reality systems to improve the usability and reduce the complexity of collaborative engineering systems. In FY 2000, we created a Tangible Reality Testbed integrating a multi-user virtual environment with remotely controllable devices. We initiated work on the recording and playback of actions in the tangible reality testbed, which will lead to a file format specification for usability studies. We developed application programming interfaces (APIs) and a Java™-based server for control and status of physical devices in collaborative environments. In addition, a file format specification for device integration is being developed to allow dynamic device configurations. The Web site is <http://ovrt.nist.gov>.

J. Garofolo and M. Przybocki discuss evaluations of speech recognition data.



High Performance Systems and Services Division Projects

Backbone Operation and Migration

At its Gaithersburg, Maryland, and Boulder, Colorado, sites, ITL is increasing network backbone bandwidth from a shared FDDI 100 Mbps system to one capable of supporting 155, 622, and 1000 Mbps switched networking. This upgrade will provide ample backbone bandwidth and Quality of Service (QoS) infrastructure to support multimedia and delay-sensitive (e.g., voice over IP [VoIP]) applications. In FY 2000, we improved service in Buildings 220, 221, and 301 in Gaithersburg by upgrading the core Asynchronous Transfer Mode (ATM) switch

to ASX-4000 and ASX-1200. We completed the DLE-based redundant ATM core and True OC-48 (2.88 Gbps) ATM implementations. Boulder improvements included the establishment of the GigaE backbone with 3 Layer-3 routers, the upgrade of the Backbone/Firewall core router from Cisco 7505 to Cisco 6505/msfc, the upgrade of the Inter-closet link from 10BaseFL to 100FX/TX, and the upgrade of the Backbone QoS capability with Cisco Catalyst 4000s. Expected completion date of the project is FY 2001.

Digital TV Application Software Environment (DASE)

Working with the Digital TV Applications Software Environment (DASE) specialist group T3/S17 of the Advanced Television Systems Committee (ATSC), ITL assists industry in developing interactive digital TV services by facilitating the development of a standard DASE Application Programming Interface (API). This will allow

B. Swope, O. Slattery, D. Kardos, B. Davis, J. Roberts, and E. Mulkens inspect the second-generation prototype of the NIST rotating-wheel Braille display.





B. am Ende, P. Ketcham, and J. Littlefield look at a 3D simulation of concrete flow.

digital TV content providers to build an application using the API, which will run on any conforming manufacturer's equipment (the TV set-top unit or STU). ITL is developing a DASE API reference implementation and supporting the development of associated conformance tests; our Software Diagnostics and Conformance Testing Division collaborates in this effort. In FY 2000, we completed a shakedown Java™ implementation of the core API specification along with emulation of the set-top unit environment. This environment provides the means to evaluate most API syntactic and semantic issues in a time frame conducive with the API specification definition process. This approach ensures that the reference implementation is as platform-independent as possible. The NIST reference implementation will include the Java™ implementation of the API specification, the simulated and emulated STU environment, sample DASE API applications, and a user's guide. We also co-sponsored with the National Information Standards Organization a Symposium on the Foundations of Interactive Digital TV Application Software Environment (DASE), held at NIST on May 23-24, 2000. The Web site is <http://www.nist.gov/itl/div895/cmr>.

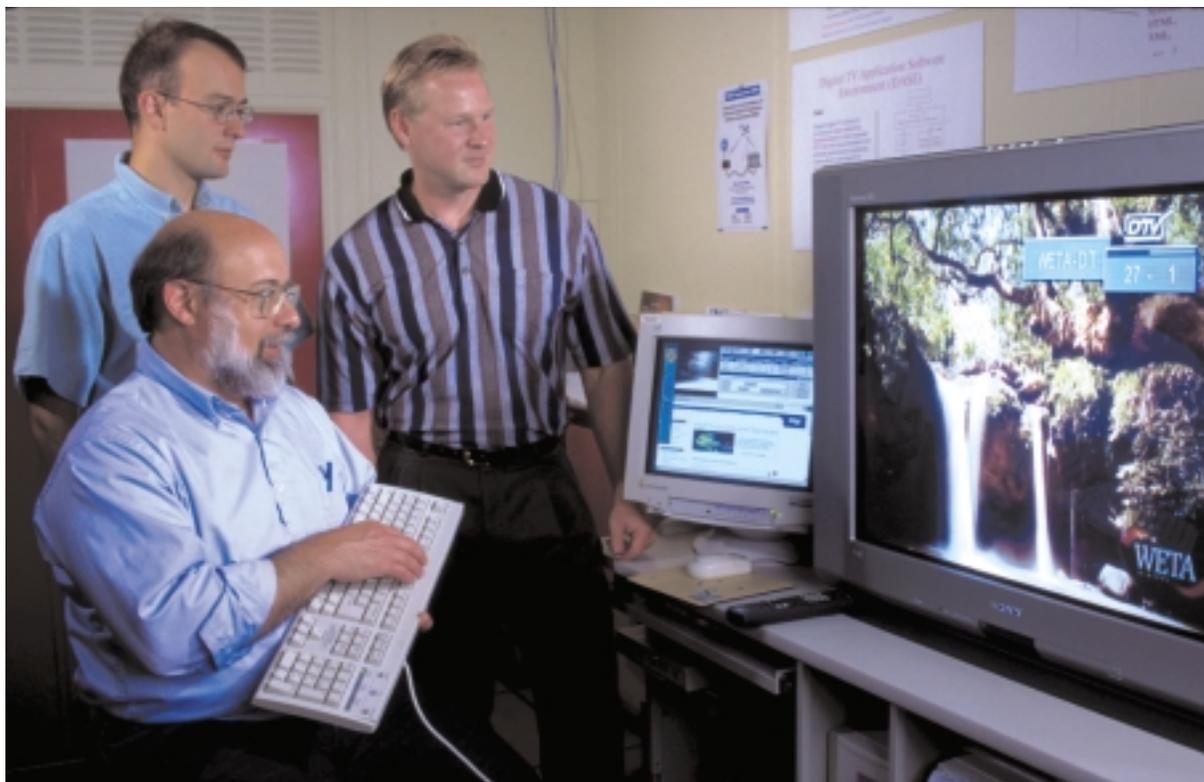
Interoperable Message Passing Interface (IMPI) and Conformance Tester

ITL is working with computer vendors to produce a standard for interoperability among different MPI implementations. The vendors

designed the standard, and ITL facilitated the effort, wrote the tests, and created a conformance tester for it. In FY 2000, we published the standard and initiated a worldwide test of IMPI. We completed the IMPI conformance tester, which is a completely Web-based system that sets up a parallel virtual machine between NIST and the testers. The conformance test suite contains over a hundred tests that exercise all parts of the IMPI protocol. This work benefits industries that use a parallel code across different vendor systems, including the embedded computing community. The Web page, <http://impi.nist.gov/IMPI>, contains the standard, the conformance tester, and pointers to the LAM implementations.

NISTnet

The goal of this ITL project is to provide common network infrastructure across the NIST campus in Gaithersburg, Maryland, and to upgrade to 10/100 Mbps network access to each office. In FY 2000, we upgraded equipment in Building 225, wired and made operational the networks in Buildings 221 and 235, and wired Buildings 223, 224, and 411. Expected completion date of the project is FY 2001.



G. Lathoud, A. Mink, and R. Snelick view a digital TV transmission while controlling a simulated TV image.

Parallel Consulting

ITL continues to provide parallel consulting services to support the scientific computing needs of the NIST staff. Our consultations with NIST clients emphasize ITL's special expertise in computational chemistry and finite-element modeling.

The Performance of Distributed Architectures

This ITL project seeks to determine and enhance the ability of networked system architectures to handle service demands arising in scientific computing, e-commerce, and other evolving inter-LAN applications. We installed, configured, and tested four PC clusters. Switched ATM (OC3) networks and switched FastEthernet networks were used to interconnect the clusters; for NIST workloads, FastEthernet is far more cost-effective with little performance difference. We used our hardware and software instrumentation to evaluate and improve the systems. We also constructed a Windows NT® cluster similar to our existing Linux system. Benchmarks and

applications were run on both environments to compare and assess their comparative strengths and weaknesses. Multiple ITL hardware-based global positioning system (GPS) time-synchronization instruments have been installed at various sites in the U.S. and France. These installations are used to assess precision of current software time-synchronization algorithms and the effects of the various limiting factors. In FY 2000, we conducted an assessment of software time-synchronization protocol precision. We also studied problems of smaller merchants and customers in pursuing effective and trusted e-commerce and published a report on assurance protocols for e-commerce.

Remote User Support

ITL is working to provide network connectivity to NIST staff at remote locations. Transparent analog and digital service will be provided to support over 4,500 users. In FY 2000, we completed the transition of 800 service from FTS2000 (AT&T) to FTS2001 (MCI). We also upgraded the ISDN infrastructure supporting modem pool and ISDN dial-in service. Finally, we established a Web-based account application for modem service. Additional service improvements will follow in FY 2001.

Distributed Computing and Information Services Division Projects

Division Office Projects

IT SUPPORT BENCHMARKING/BALDRIGE EVALUATION: ITL is using the Baldrige Quality Criteria and industry benchmarking to perform a self-assessment in order to provide a framework for performance excellence within the organization. In FY 2000, the PC Support group re-examined its procedures and performed benchmarking exercises with government and industry PC support organizations.

CENTRALIZED HELPDESK: To respond to the need to provide "best-in-the-world" service to NIST staff, we reviewed establishing a

P. Feulner, A. Ashcraft, and T. Antonishek monitor the performance of desktop PCs on the NIST internal network.

centralized helpdesk. In FY 2000, we conducted a survey of existing "helpdesks" and telephone hotlines to determine the nature and volume of the existing workload. We then prepared an initial proposal for funding for the renovation of office space and the use of contractor personnel to staff the helpdesk. The centralized helpdesk will be implemented in 2001.

Distributed Processing and Operating Systems Support Projects

UNIX SERVER/WORKSTATION SUPPORT: To meet the needs of the NIST staff, ITL operates and maintains the central NIST servers and supports scientific workstation computing software and hardware. In Gaithersburg and Boulder, central services such as electronic





H. Cox (Conference Facilities), G. DeConti, and J. Porterfield set up equipment for a Webcast.

mail, calendaring, electronic mail list processing, and file services are supported. Services are expanded and enhanced as needed. A more specialized service provided by the group is software check-out, where licensed software packages are made available. In addition, the group administers, on a fee basis, users' Sun™, Silicon Graphics®, and, in Gaithersburg only, Red Hat Linux workstations.

ENTERPRISE E-MAIL CENTRALIZATION: To better serve our NIST customers, ITL is enhancing the NIST electronic mail system by transitioning to the IMAP protocol from the POP3 protocol. One advantage to IMAP is that it uses less network bandwidth. In FY 2000, we installed the new e-mail server and began to transition users from POP to IMAP.

WINDOWS NT® SUPPORT INITIATIVE: ITL provides support for Windows NT® customers with a Windows NT® service team. Important outcomes of this initiative include the definition of an architecture that ensures that servers are introduced, named, and connected in an orderly manner, that the latest trust and security protection techniques are utilized to ensure optimum operation, and that workstations are properly set up to provide the flexibility required by NIST users. The team also provides support to Windows NT®-based Web servers. In FY 2000, we began server implementation of Windows® 2000 for our NIST customers.

THIN CLIENT INITIATIVE: To make applications available to a wide spectrum of NIST clients quickly while keeping application maintenance costs to a minimum, ITL implemented a scalable Windows NT® server farm for hosting thin client applications. The farm currently consists of four Compaq Proliant 8500R servers. In FY 2000, we developed the CSTARs Procurement System and the Pay for Performance System for implementation on the Windows NT® server farm and distribution to NIST staff.

COMPUTER SECURITY INITIATIVE: To assist the NIST staff when computers are compromised, ITL created a team to help users recover from intrusions and configure their machines so they are as secure as possible. To date, the team has responded to approximately 30 incidents. We developed security checklists for UNIX and Windows NT® computer systems. We also assist the administrators of NIST central servers with security vulnerabilities and provide information to help NIST system administrators to keep current on patches for security vulnerabilities. On an ongoing basis, we conduct vulnerability analyses of systems as requested, as well as develop and offer computer security training for NIST staff.

Information Processing Support Projects

WEB/INTERNET SERVICES: ITL operates and maintains the central NIST Web servers. We set up publicly accessible Web and ftp servers with the necessary resources to accommodate over 135 gigabytes of Web documents and 17 gigabytes of ftp documents. This involved creating more than 35 virtual Web servers to enable customers to retain their domain names. We developed a procedure that pushes the publicly accessible files from the NIST private server (not publicly accessible) to the NIST public server at set time intervals. In addition to providing ongoing system administration, system architecture, and infrastructure support to Web administrators throughout NIST, we provide Web database support and general Web consulting services to the NIST user community.

ELECTRONIC APPROVAL: The purpose of this project is to automate the electronic routing and approval of selected internal NIST processes. We conducted an initial assessment of electronic approval technologies and evaluated several candidate solutions. In April 2000, we awarded a contract to MATCOM Inc. to implement electronic approval at NIST. We implemented an initial pilot test of 100 seats, using NIST's intranet and, as much as possible, commercial off-the-shelf (COTS) products, i.e., electronic forms, a workflow solution, and a digital signature public key infrastructure. Upon successful completion of the pilot, we will implement the 3000-seat system.

WEBCASTING: To respond to user demand, ITL provides routine webcasting service of NIST events to NIST staff. In FY 2000, we began webcasting non-ITL conferences, NIST town meetings, and program reviews for other NIST laboratories. We upgraded webcasting equipment to support full-screen, 30-frame-per-second, DVD-quality transmissions. Finally, NIST entered into an inter-agency webcasting agreement with other federal agencies.

ITL Web Support: We support Web and multimedia activities for ITL. To enhance ITL's Website, we developed preliminary redesigns, including an ITL logo and other related identity pieces. We met with the ITL division chiefs to collect their input. In FY 2000, we worked with ITL management to fine-tune the selected design and add desired functionality prior to releasing the new Web page. We also provided multimedia support to the ITL laboratory office and divisions.

Administrative Computing Support Projects

ADMINISTRATIVE APPLICATIONS DEVELOPMENT: To respond to the need for development and support of NIST administrative software applications, ITL develops and maintains central administrative applications, including the financial systems, human resources, property, and procurement. On an ongoing basis, we support administrative application software and systems for both PCs and central systems. In addition, we provide training and consulting with administrative users on the design and implementation of new administrative systems.

COMMERCE ADMINISTRATIVE MANAGEMENT SYSTEM (CAMS): The purpose of the CAMS project is to implement the Core Financial System software for the Department of Commerce (DoC) Office of the Secretary and eventually for use at NIST. We set up database servers to support implementation for the DoC Office of the Secretary. We provided database administration support in setting up the core financial system software and staging areas. Finally, we began to prepare the communications for access by DoC staff via the FNS network.

COMMERCE STANDARD ACQUISITION REPORTING SYSTEM (CSTARS): NIST is the pilot agency within the Department of Commerce (DoC) for implementation of the CACI/COMPRIZON.BUY Procurement Automation System. Upon the successful implementation of the system at NIST, other DoC agencies will follow, starting with the Office of the Secretary. DoC awarded to CACI a contract to purchase the SACONS software and develop a full project plan. The implementation start date was February 1, 2000. We implemented the IT infrastructure to host the new system and started the design of the interface requirements to our existing system.

GRANTS MANAGEMENT INFORMATION SYSTEM: This project seeks to improve the management of grants at NIST and to develop a central repository for management reports. In FY 2000, ITL awarded the contract for the development of the system and completed the design specifications and functional requirements. We also provid-

ed consulting services regarding the IT infrastructure and security.

NON-EMPLOYEE INFORMATION SYSTEM: To respond to the need to automate the administrative processes related to non-employee NIST workers, i.e., guest researchers and contractors, ITL is developing an automated, Web-based system to provide support for the administrative processes associated with non-employee NIST workers. In FY 2000, we developed a pilot system and implemented it for both foreign and domestic guest researchers. Next year, we will expand the system to include contractors.

PERFORMANCE PAYOUT SYSTEM: The goal of this project is to implement a Windows[®]-based, Web-accessible performance payout system. In FY 2000, ITL assisted in the identification of changes required to the existing system. We provided consulting services and assisted in designing a new system to interface with existing NIST human resources systems. The initial transfer of data using the new system will occur in 2001.

PC Support Projects

MANAGED DESKTOP: ITL seeks to utilize emerging technologies to provide customer support and to implement central procurement, upgrade, and management services for desktop computers at NIST. In FY 2000, we set up a laboratory and acquired different vendor equipment, hardware, and software, in order to begin testing the desktop management capabilities of each vendor's product. We worked with procurement personnel to explore methods for acquiring the hardware for the PC Buying Service. We also created and tested a Web site that will automate the purchase of standard hardware and software and the backend accounting function. We implemented a software install wizard via NIST's internal Web. We provided a mechanism to enable NIST staff to purchase software that is not site-licensed. Finally, we explored remote control technologies and developed an internal seat management plan.

TRAVEL MANAGER: The objective of this project is to provide NIST staff with a travel system that automates the creation of travel authorizations and vouchers, thus increasing the percentage of vouchers that pass audit, and to reduce the time taken to process travel requests through the implementation of electronic routing. Travel manager became mandatory at NIST in 1998. In FY 2000, we implemented a pilot electronic routing, began to phase in the electronic routing system, and interfaced Travel Manager with the NIST Travel Payments System. The electronic routing implementation will be completed in 2001.

Software Diagnostics & Conformance Testing Division Projects

Architectural Description Languages for Component-Based Software Development

ITL is working with the software industry and research communities on the standardization of an Architectural Description Language (ADL), which is a computer-readable language for rigorously defining a software systems architecture. In FY 2000, we collaborated with the Society for Automotive Engineers AS-5A Avionics Architectural

Description Language Task Group to ensure that necessary functionality is specified, including conformance testing to determine compliance of system designs with reference architecture. We identified domain areas for applying ADL to explore standardization and testing issues (e.g., government smart card, unmanned ground vehicle, pervasive computing). Finally, we explored standardization efforts in the Institute of Electrical and Electronics Engineers and the Open Group.

Aroma Pervasive Computing Project

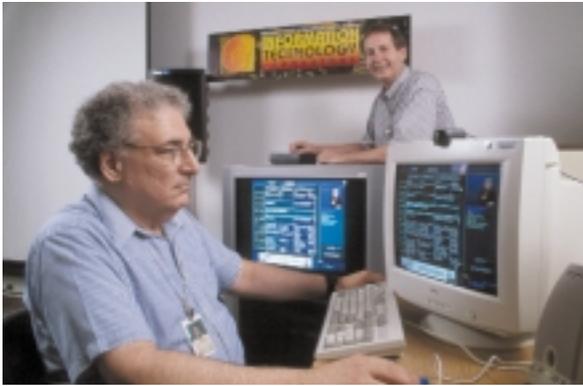
Working with industry, ITL is developing a conceptual model for describing pervasive computing. In FY 2000, we co-chaired the NIST Pervasive Computing 2000 Conference. We developed a conceptual model for pervasive computing inspired by the OSI Reference Model. We collaborated with the U.S. Naval Academy to build low-end microcontroller-based hardware/software platforms for pervasive computing. With the Advanced Network Technologies Division, we developed and conducted performance measurements of Aroma Adapter-Projector using embedded PC technology, Java™, Jini™, and Linux. The Web site is <http://www.nist.gov/aroma>.

Automatic Generation of Tests from Formal Specifications

This ITL project harnesses formal methods to improve the quality of software by automatically generating tests for software from formal specifications. To date, we have developed a method for automatically generating tests from formal specifications, developed a coverage metric for the method, developed a method of abstracting formal specifications so that model checkers may be applied, and worked with industrial collaborators to demonstrate

M. Brady and R. Rivello discuss XML-related technologies.





A. Goldfine and J. Barkley develop conformance test methods for interactive TV.

the feasibility of the automatic test generation method. Ford Motor Company and Argus Security collaborate on validating the NIST method of automatic test generation. See <http://hissa.nist.gov/~black/FTG/autotest.html>.

Healthcare Information Systems

ITL is assisting the Department of Veterans Affairs (VA) in making informed decisions with regard to technology choices for their healthcare information system VistA. We are designing distributed models and architectures for VistA and developing reference implementations for these designs. In FY 2000, we designed and implemented the prototype Inter-Organizational Role Based Access Control (IORBAC) authorization mechanism. In addition, we participated with other federal agencies in the development of standards in the healthcare industry. See <http://www.nist.gov/va/>.

Interactive TV

Interactive TV is an important new electronic commerce initiative that is developing standards that enable the seamless convergence of two currently separate media, broadcast TV and the Internet. The Digital Application Software Environment Committee (DASE), within the Advanced Television Standards Committee (ATSC), along with the Declarative Data Essence Group (DDE) of the Society for Motion Picture and Television Engineers (SMPTE), are developing the needed standards. In FY 2000, we ensured that effective conformance statements were included in the DASE specification and reviewed the test assertions and conformance tests developed by UniSoft. We also contributed text to the DDE specification, devel-

oped conformance tests for the trigger and binding elements of the DDE specification, and initiated the development of a DDE testbed. The Web site is <http://www.nist.gov/itl/div897/ctg/dase/daseprojectwebpage.htm>.

Learning Technologies

In collaboration with industry, government, and standards groups, ITL is defining requirements and developing specifications, prototype demonstrations, and testing techniques for object technology and metadata that enable the development of distributed, interactive learning systems. In FY 2000, we developed a conformance testing plan for Instructional Management System (IMS) specifications, finalized a security architecture for IMS systems, chaired IMS conformance testing activities, and developed a repository of learning objects, including a metadata vocabulary to reflect the IMS metadata standard. The Web site is <http://www.itl.nist.gov/div897/ctg/projects.htm>.

National Software Reference Library (NSRL) and Computer Forensics Tools Verification

The NSRL project establishes a baseline of known file profiles and signatures that can be used as a reference data set in legal proceedings concerning criminal evidence investigation, software piracy, copyright infringement, and child pornography. The Computer Forensics Tools Verification project provides a testing framework and procedures for independent laboratories to verify computer forensics tools capabilities. In FY 2000, we developed prototype software to create reference data sets through manual application, reference data set entries, and a testing framework for computer forensics tool testing. We also determined the validity of selected computer forensics tools based on our testing framework. Collaborators include the National Institute of Justice, the Defense Computer Forensics Laboratory (DCFL), the Federal Bureau of Investigation's Computer Analysis Response Team (CART), Microsoft Corporation, Adobe Systems, Inc., and other state and national groups. The Web site is <http://www.nsr1.nist.gov>.

Quantum Information

In a joint project with NIST's Physics Laboratory, ITL is developing information representations and computing machines that take advantage of quantum effects, such as superposition and entan-

gment, which could enable exponential computational work to be done in one operation. In FY 2000, we attended weekly Physics Quantum Information seminars and presented the Basic Concepts in the Theory of Computation to colleagues in the Physics Laboratory. We developed a Quantum Information Demonstration and a Quantum Information Bibliography. We participated in developing a joint proposal for a Nanotechnology Initiative with the Physics Laboratory. Finally, we initiated Quantum Information seminars in ITL.

Software Testing by Statistical Methods

This NIST competency project seeks to improve the development and measurement of software testing by applying statistical methods. In FY 2000, we developed a statistical approach for coverage metrics applied to mutation testing. We continued work on the reliability of conformance test suites and object-oriented components. Finally, we investigated the use of statistical methods in pervasive computing technologies. The result of this effort will be new paradigms for software testing that are more efficient and less labor intensive than traditional methods.

See <http://www.nist.gov/stsm.html>.

Guest researcher L. Ciarletta and Aroma project leader A. Dima demonstrate their remote smart projector.



XML/DOM Conformance Testing

In partnership with industry, ITL is developing conformance tests for the Extensible Markup Language (XML), which provides a standards-based approach to universal methods for defining and exchanging data. The Document Object Model (DOM) defines ECMAScript and Java™ bindings for interacting with both XML and HTML data, permitting dynamic creation and manipulation of Web pages defined using these metalanguages. In FY 2000, we chaired the Organization for the Advancement of Structured Information Standards (OASIS) Conformance and XML Testing Committees. We completed the XML Test Suite, releases 1 and 2. We also completed the DOM ECMAScript Test Suite and the DOM Java™ Test Suite. Finally, we provided conformance expertise to the ebXML Initiative. See www.nist.gov/xml/.

XML Registry and Repository Interfaces

ITL seeks to influence the quality, correctness, and testability of the specifications of both the OASIS and ebXML Registry/Repository Working Groups through our reference implementation of a registry and repository that is conformant to both specifications. In FY 2000, we chaired the OASIS Registry/Repository Working Group. We developed a draft OASIS Registry/Repository Specification and Version 1 of the Reference Implementation for the OASIS Registry/Repository Specification. We contributed to the ebXML Registry/Repository Specification. Finally, we coordinated the efforts of the OASIS Registry/Repository Working Group and the exXML Registry/Repository Project Team so that the resulting specifications are compatible. The Web site is <http://www.nist.gov/itl/div897/ctg/regrep/index.html>.

Other Division Projects:

- Error, Fault, and Failure Data Collection and Analysis
- Integrated ISO GIS Standards for Industry
- Java™ Testing Project
- Metadata Descriptions and Registries
- Requirements Collection for Forward-Looking Standards
- Technology Transfer of Conformance Testing Programs
- Unravel
- VRML and X3D Conformance Testing
- XSL Conformance Testing

Statistical Engineering *Division Projects*

Bayesian Metrology

Bayesian methods provide a unified framework for optimally combining information from multiple sources, resulting in simpler and improved statistical analyses. A joint venture involving ITL, the Physics Laboratory, and the Manufacturing Engineering Laboratory, this five-year NIST competence initiative focuses on the research, development, and application of Bayesian techniques to NIST research in metrology and the transfer of findings to other metrology laboratories. Selected because of their importance to NIST researchers and the potential benefit of Bayesian methods to these researchers, the areas of traceability, interlaboratory comparisons, calibration, and part inspection form the nucleus of the project. In FY 2000, we researched Bayesian hierarchical models and Bayesian computation. We developed and refined Bayesian methods for the certification of Standard Reference Materials (SRMs). We also solved case study applications of Bayesian methods at NIST and explored the use of objec-

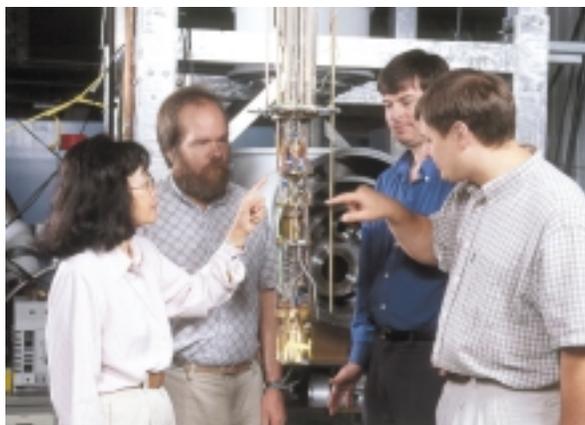
tive prior distributions. Upon completion of this project, NIST products and services, such as SRMs, calibrations, and key comparisons, will have higher-quality uncertainty estimates, resulting in greater utility for NIST customers.

Collaborative Research with NIST Scientists and Engineers

For more than 50 years, Statistical Engineering Division staff has played a critical role in the success of a broad spectrum of interdisciplinary collaborative research projects at NIST. As members of interdisciplinary teams, division staff members develop appropriate statistical strategies to meet the needs of the research team. In

M. Vangel of the Statistical Engineering Division consults with M. Schantz of the Analytical Chemistry Division on the data of a Standard Reference Material (SRM).





G. Yang and K. Coakley of the Statistical Engineering Division collaborate with P. Huffman and S. Dewey of the Ionizing Radiation Division on experimental determination of the mean lifetime of magnetically trapped ultra cold neutrons.

some cases, the statistician judiciously selects and implements the most appropriate existing statistical method to analyze experimental data. In many cases, new statistical methods are developed to address unique scientific challenges encountered by the NIST research team. Statisticians often participate in the planning of experimental studies and conduct rigorous and nontrivial uncertainty analysis of results. Some division staff members develop theoretical models to augment experimental work done by NIST collaborators. Examples of such work include Monte Carlo simulation of physical processes and stochastic differential equation modeling. Many U.S. industries benefit from this work, including the building and construction, steel, opto-electronics, computer hardware and software, biotechnology, polymer, semiconductor, wireless communications, and cable television industries.

Key Comparisons and International Interlaboratory Studies

Interlaboratory studies have long been used to ensure measurement capability for commerce since accurate measurements are necessary for assessing product specifications. For this reason, design and analysis of interlaboratory studies have been an important part of the division's work for many years. Recently, a new type of interlaboratory study, known as a key comparison, has taken a critical new place in the NIST mission. In the last year, key comparisons, which are international interlaboratory studies for comparing measurement results between leading National Metrology Institutes (NMIs), have provided many new opportunities for ITL statisticians to collaborate with NIST scientists. The

impetus for these new opportunities is a Mutual Recognition Arrangement (MRA) signed in FY 2000 by the NMIs belonging to the International Committee for Weights and Measures (CIPM) "to establish the degree of equivalence of national measurement standards maintained by NMIs, to provide for the mutual recognition of calibration and measurement certificates issued by NMIs, [and] thereby to provide governments and other parties with a secure technical foundation for wider agreements related to international trade, commerce and regulatory affairs." ITL collaborates with six other NIST laboratories in the key comparison endeavor.

Key comparisons serve as the technical basis for the MRA and must therefore accurately reflect the true relationships between measurement systems maintained by NMIs belonging to the CIPM. The results of key comparisons must also be extensible to members of Regional Metrology Organizations (RMOs) to maximize recognition of measurement capabilities that exist in other metrology laboratories around the world. In FY 2000, we completed an analysis of key comparison data and wrote draft reports. We planned and initiated an experiment design for additional key comparisons. We also published final reports for our first key comparisons. The results of each comparison are available in the BIPM Key Comparison Database at http://www.bipm.fr/enus/8_Key_Comparisons/database.html.

NIST/SEMATECH Engineering Statistics Internet Handbook

In collaboration with SEMATECH, a consortium of major U.S. semiconductor manufacturers, ITL is developing an online Handbook of Engineering Statistics to provide modern statistical techniques and examples related to the semiconductor industry. The purpose of the project is to extend the benefits of modern statistical design and analysis to the engineering and scientific communities and contribute to the productivity and competitiveness of U.S. industry in world markets. The approach is problem-oriented and includes detailed case studies from the semiconductor industry and the NIST laboratories that illustrate statistical approaches to solving engineering and scientific problems. Distributed freely on the Web, the handbook is integrated with a free, down-loadable statistical analysis package, Dataplot, maintained by ITL. During FY 2000, we completed chapters on Production Process Characterization, Process Modeling, and Process/Product Improvement. We edited the final product, put together case studies with interactive com-



Staff of the Statistical Engineering Division collaborate on key comparisons with scientists from all the NIST Laboratories. Pictured here are W. Guthrie and M. Levenson reviewing some of the key comparison reports to which the division has contributed.

putational capabilities, and developed a system for revising and updating the document. The Web site is <http://www.itl.nist.gov/div898/handbook/index.html>.

Research on Statistical Methods

The primary objective of this project is to ensure that appropriate, state-of-the-art statistical planning and analysis are used in NIST work. The project produces novel statistical procedures for NIST problems that do not satisfy the prerequisites of existing statistical methods. Because such research will have valid applications elsewhere, both at NIST and in many industries, the work conducted under this project is presented in archival journals of statistics. The emphasis in reporting research is on the broadly applicable statistical methods, discovered and developed in the course of a particular need and application. The division typically produces several publications on new statistical methods each year.

An example project is the Statistical Process Monitoring and Control for Correlated Data. This project seeks to provide new statistical measures and techniques for process monitoring and control in manufacturing industries and for other applications, such as Internet traffic monitoring and scanning electron microscopy (SEM) linewidth measurement process control. The goal of this research is to provide more efficient process control charts and other monitoring tools, including process capability indices, for correlated data. In FY 2000, we published a paper on the comparisons of control charts for autocorrelated data and

proposed the use of generalized moving averages of stationary process data to reduce process autocorrelations. Two other NIST laboratories applied the uncertainty calculation to the averages of the linewidth measurements. By using this method, better estimates of uncertainty of measured linewidths were obtained.

Statistical Education

Education of the NIST staff is a core component of the division's service, consulting, communication, and research mission. All of these scientific-method components benefit from both general and NIST-specific statistical principles and techniques developed over the years in conjunction with division staff expertise and experience. NIST has over 1300 scientists and engineers who are formulating investigations, planning experiments, collecting data, analyzing data, and deriving scientific and engineering conclusions. The objective in statistical training is to assure valid, supportable, repeatable scientific and engineering conclusions while maximizing insight and minimizing time and cost. The understanding of statistical methods and uses by the NIST technical staff results in greater efficiency, cost savings, and insight, thereby improving NIST products. The division uses several different education forums, including short courses (on-site and off-site) on specific topics (e.g., experiment design, uncertainty analysis); a series of short courses on a variety of topics (e.g., the Statistics for Scientists series); and Web-based training material (e.g., the NIST/SEMATECH Engineering Statistics Handbook).

INDUSTRY INTERACTION

INDUSTRY INTERACTIONS

ITL partners with industry, academia, and government to pursue research areas of mutual interest. Through Cooperative Research and Development Agreements (CRADAs), we worked with 20 organizations in FY 2000. In addition, we participated in many consortia and industry interest groups, including the following:

J. Wang, T. Clement (EEEL), P. Hale (EEEL), and K. Coakley develop methods for characterizing high-speed optoelectronic devices. These devices play a critical role in optical communications systems.

PAGE

30

TECHNICAL ACCOMPLISHMENTS

ITL



Advanced Television Systems Committee (ATSC)

The ATSC establishes voluntary technical standards for advanced television systems, including digital high definition television (HDTV). ITL staff members Alan Mink, Robert Snelick, Wayne Salamon, Alan Goldfine, Mark Skall, and Lynne Rosenthal participate in T3/S17, Digital TV Applications Software Environment (DASE) Application Programming Interface (API).

Air Transport Association (ATA) and Aerospace Industries Association (AIA)

The ATA and AIA are international nonprofit organizations for the airline industry and aerospace suppliers. The ATA, AIA, and ITL are working together to develop a graphics profile and conformance tests methods for the interchange of graphics data within the commercial aerospace industry. Lynne Rosenthal is the ITL contact.

American National Standards Institute (ANSI)

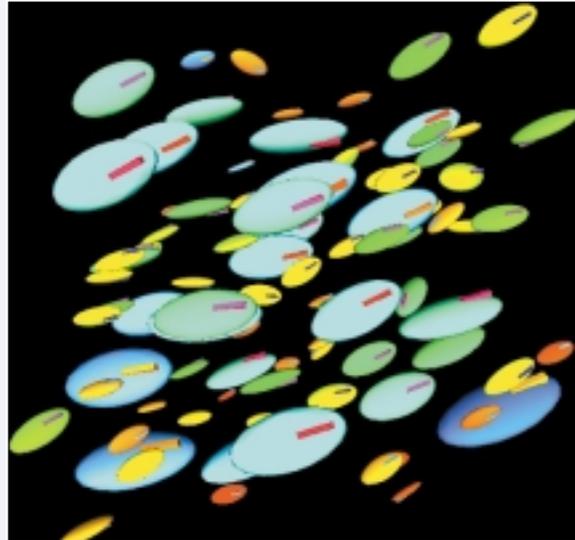
ANSI has served in its capacity as administrator and coordinator of the United States private sector voluntary standardization system for 80 years. Michael Hogan participates on the ANSI Information Systems Standards Board (ISSB). NIST/ITL is an ANSI-accredited standards developer. Michael McCabe is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

American Society of Quality (ASQ)

The American Society of Quality advances individual and organizational performance excellence worldwide by providing opportunities for learning, quality improvement, and knowledge exchange. Carroll Croarkin participates on the Statistics Subcommittee (ISO TC 69 Statistical Methods).

Association for Computing Machinery (ACM)

ACM is the world's oldest and largest educational and scientific computing society. Since 1947, ACM has provided a vital forum for the exchange of information, ideas, and discoveries. Ronald Boisvert serves on the ACM Publications Board; John Barkley participates in the Role Based Access Control working group.



This image shows the motion of a suspension of ellipsoidal objects under shear. The simulation is based on a dissipative particle dynamics (DPD) algorithm written at NIST. The DPD program determines the viscosity of the suspension as a function of shear rate and particle size and shape distribution. The DPD model is being developed to help predict the rheological properties of cement-based materials. The numerical simulation was done by Nicos Martys of BFRL with parallel programming support by Jim Sims of ITL. The graphics conversion of the resulting data to Virtual Reality Modeling Language (VRML) was done by Steve Satterfield. Use of VRML allows the visualization to be widely distributed to anyone with access to the Internet.

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, Committee C21, Advanced Data Storage Subsystems, and three related subcommittees.

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. Carroll Croarkin participates in Technical Committee E-11, Quality and 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 kernel and extending the BLAS to new domains. This work includes the development of interface specifications, reference implementations, and a project Web site. Roldan Pozo chairs the sparse matrix subcommittee.

BioAPI Consortium

The Biometric Application Programming Interface (API) Consortium serves as the federal government's focal point for research, development, test, evaluation, and application of biometric-based personal identification and verification technology. Fernando Podio serves on the Steering Committee and the External Liaisons Working Group.

CommerceNet Consortium

CommerceNet is an industry association for Internet commerce whose mission is to make electronic commerce easy, trusted, and ubiquitous. ITL is one of 500 members of the organization. Bruce Rosen represents ITL in the association and Tom Rhodes participates in the eCo Framework Working Group.

Cross Industry Working Team (XIWT)

The XIWT is a multi-industry coalition committed to defining the architecture and key technical requirements for a powerful, sustainable national information infrastructure (NII). Kevin Mills represents NIST on the executive committee.

DVD Forum

The Digital Versatile Disc (DVD) Forum promotes the implementation and standardization of this data storage technology. Xiao Tang represents ITL on the Working Group on Data Format.

Electronic Book Exchange (EBX)

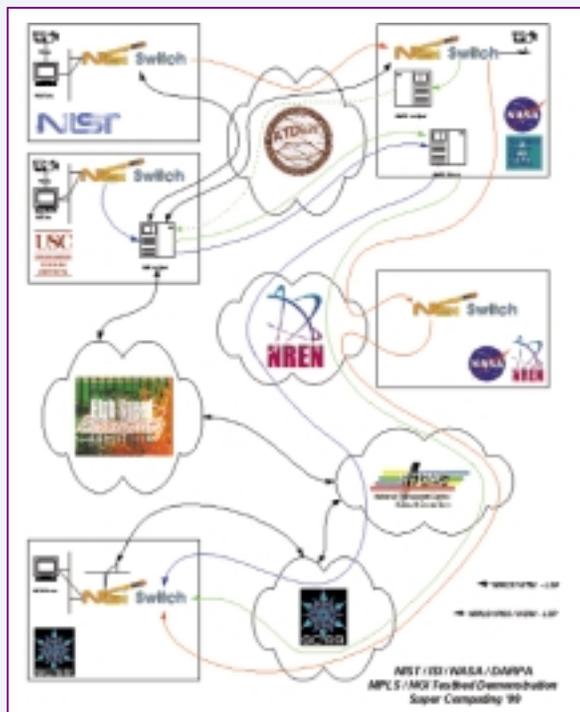
EBX is focused on providing intellectual property protection for the e-Book industry. NIST participates as a team member with technical support for the project. ITL chairs the authoring group for the Open e-Book Initiative, an industry group focused on developing a standard for electronic content on electronic book reading systems. In addition to representing ITL in EBX, Victor McCrary participates on the Japanese Electronic Book Consortium Steering Committee.

ECMA

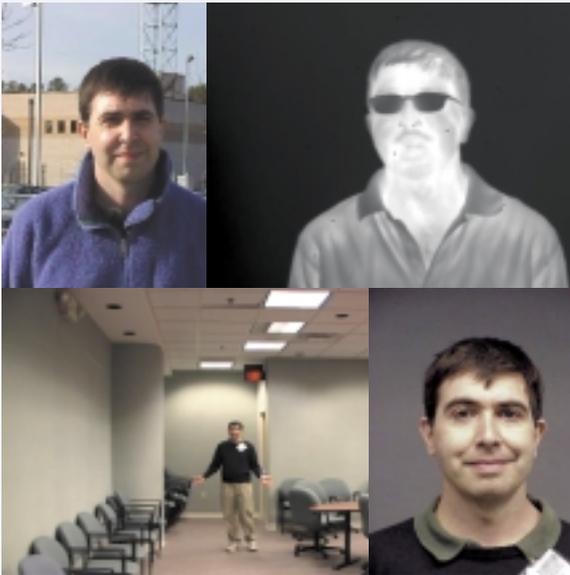
ECMA is an international, Europe-based industry association founded in 1961 and dedicated to the standardization of information and communication systems. Gary Fisher participates in TC39, Scripting Languages.

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. ITL, with support from



The many faces of human identification. Pictured is Jonathan Phillips appearing in real world variations of human images that need to be addressed by automatic identification algorithms. Clockwise from top left is a photo taken outdoors showing non-uniform shadow effects, an infra-red image, a portrait of a cooperative individual taken under reasonably controlled conditions, and photo of a subject at a distance from the camera.



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. Arnold Johnson represents ITL.

IMS Global Learning Consortium

IMS is a consortium of university and industry providers of educational material. ITL provides leadership to the Instructional Management System (IMS) in its development of standards and conformance test methods. Mark Skall serves on the IMS Advisory Board; Tom Rhodes serves on the Technical Board.

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 VanDyck, 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.

Interoperable Message Passing Interface (IMPI)

ITL actively participates in the development of standards and testing for IMPI. William George, John Hagedorn, and Judy Devaney represent ITL.

International Standards Organization (ISO)

Christopher Dabrowski participates in ISO TC211 WG1, Framework and Reference Model, as the Working Group Convener.

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. ITL participates in Audio/Video Transport, the Internet Area, IP over Optical Networks, the Management Area, Multiparty Multimedia Session Control, the Operations and Management Area, the PKI Using X.509 Working Group, the Routing Area, the Security Area, the S/MIME Working Group, and the Transport Area. Doug Montgomery is the principal ITL contact.

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.

Java™ Grande Forum

The Java™ Grande Forum (JGF) is an open forum of industrial, government and academic researchers, and software developers interested in improving the Java™ language and environment for use in high performance computing. Roldan Pozo and Ronald Boisvert co-chair the Numerics Working Group.

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.

Micromagnetic Modeling Activity Group (muMAG)

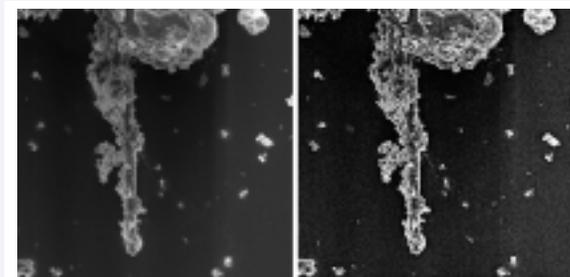
muMAG is an organization of industrial, government, and academic researchers investigating fundamental issues in micromagnetic modeling through the establishment of standard problems for testing micromagnetic simulation software and the development of a public domain reference implementation of micromagnetic 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 the areas of multimedia (MPEG/JPEG), intercommunication among computing devices and information systems (including the Information Infrastructure, SCSI-2 interfaces, Geographic Information Systems), storage media (hard drives, removable cartridges), database (including SQL3), security, and programming languages (such as C++). Michael Hogan serves on the NCITS Policy and Procedures Committee. ITL staff participate in many technical working groups in this organization. Participation in management activities includes David Su and David Cypher in T1, Telecommunications.

North America OpenMath Initiative (NAOMI)

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



ITL mathematician Alfred Carasso has developed a very efficient technique for blind image deconvolution. Using this technique, the blurred scanning electron microscope image of a dust particle generated by the Microanalysis Group in the NIST Physics Lab (left) is restored (right). The procedure is "blind" because the cause of the blur is unknown.

organization.

OASIS

OASIS, the Organization for the Advancement of Structured Information Standards, 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.

Object Management Group (OMG)

The 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 was established to aid in 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 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. The group is basing its work on the NIST publication Requirements for Real-Time Extensions for the Java™ Platform. Alden Dima represents ITL on the expert group.

Smart Card Security Users Group (SCSUG)

Organized in 1999 under the sponsorship of the National Information Assurance Partnership (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®. Eugene Troy organized and chairs the informal consortium.

M.Ting, T. Perkins, and Y. DiCarlo successfully test voice calls over IP network between Boulder IP routers/switches and Meridian PBX.



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 Alan Goldfine participate on the Committee on Data Essence Technology, and Randall Easter attends the Study Group on Conditional Access for Digital Cinema.

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.



Fern Hunt ITL is coordinating the development of a computer rendering system that utilizes high-quality optical measurements to generate photorealistic images. This image, rendered by Gregory Ward Larson of Silicon Graphics, utilizes NIST measurements of surface reflectance from the NIST Physics Lab.

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. As a member of VESA, ITL participates in the technical development of standards and develops laboratory implementations of proposed interface architectures and develops metrics. John Roberts represents ITL on four committees in this organization.

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. Michael Kass 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. Wo Chang, Lisa Carnahan, and Mary Brady represent ITL.

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 and James Foti participate 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. James Foti and Elaine Barker attend X9F.3, Cryptographic Protocols, and Annabelle Lee participates in X9F.5, Digital Signature and Certificate Policy.

INTERNATIONAL ACTIVITIES

Egyptian National Institute for Standards Collaboration.

ITL is developing a database of software faults and failures to help the software industry identify the types of faults that occur in different kinds of software. In FY 2000, a guest researcher from the Egyptian National Institute for Standards (NIS) worked with ITL to develop an Arabic language version of the database and tools that will help to improve quality and productivity in the Egyptian software industry. Larry Reeker is the ITL contact.

networks that will be employed within critical information infrastructures in the future. Conference highlights included the signing of the International Common Criteria Recognition Arrangement by the United States, Canada, Australia, New Zealand, the United Kingdom, France, Germany, the Netherlands, Finland, Norway, Italy, Spain, and Greece. The 13 nations agreed to accept the computer security testing results conducted in each others' accredited testing laboratories, thus greatly reducing the time and cost of security evaluations and increasing the availability of evaluated products for consumers. Ron Ross organized the conference for ITL.

First International Common Criteria Conference

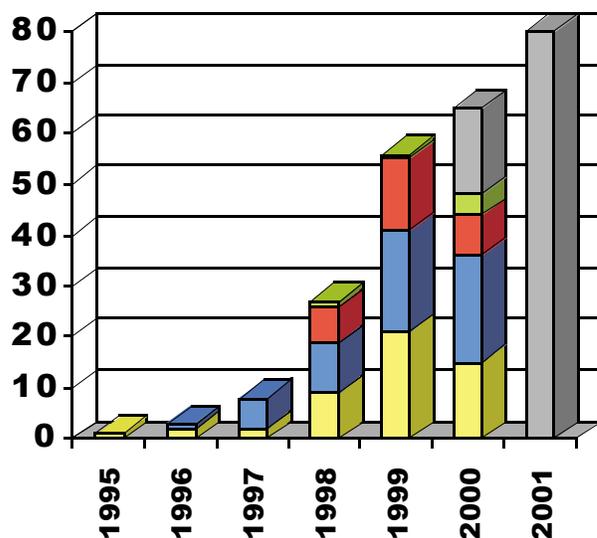
Six hundred people from 23 nations gathered in Baltimore, Maryland, on May 23-25, 2000, to participate in the First International Common Criteria Conference. Sponsored by the National Information Assurance Partnership (NIAP), the historic event brought together government and industry representatives from around the world to discuss the types of security features and assurances needed in commercial products for the systems and

G8 Information Society Projects

The G8 Global Marketplace for Small and Medium Enterprises (SMEs) project, which started in February 1995, has successfully completed its pilot phase. When the project started, very few people recognized the importance that the Internet would have on electronic commerce. We aimed to help SMEs' participation in global trade by using the new open networks. We also stressed the importance of close cooperation between industry and the public

FIPS 140-1 Validated Modules by Year and Level

(as of October 18th, 2000)



- ▣ Projected
- ▣ Level 4
- ▣ Level 3
- ▣ Level 2
- ▣ Level 1

sector in achieving this goal. The G8 project, co-chaired by Judi Moline (United States), Yoshitaka Toui (Japan), and Rosalie Zobel (European Commission), was the first important public initiative in international electronic commerce. It was catalytic in stimulating worldwide policy dialogue and providing practical help for SMEs in this area.

The G8 Global Inventory Project (GIP) was launched in 1995 and has completed its pilot phase under the leadership of the European Commission and Japan. Judi Moline served as the U.S. contact. The GIP's internationalization efforts included defining common protocols, making information accessible to all in many languages, and expanding its project boundaries worldwide beyond the G8 to include the participation of non-G7/G8 countries and NGOs (Korea, PICTA, Bellanet, Global Bangemann Challenge, ETHOS, and ACTS). At the international level, the GIP provided a forum for information exchange that fostered alliance-building opportunities for the development of Information Society applications.

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. In October 2000, WG2.5 hosted a Working Conference on the Architecture of Scientific Software in Ottawa, Canada. Ronald Boisvert, who represents ITL, chairs WG2.5 and co-edits the conference proceedings, which will be published by Kluwer Academic Press in 2001.

International Y2K Cooperation

During the millennium rollover period between Christmas 1999 and the first business day of 2000, ITL provided support to the United Nations-sponsored International Y2K Cooperation Center (IY2KCC). The center operated in conjunction with the Federal Y2K Information Collection Center. The IY2KCC monitored the rollover as it occurred in each time zone from New Zealand through Hawaii. The center received and validated reports on the status of a dozen infrastructure sectors from national coordinators in 150 countries. Dennis Steinauer, Computer Security Division, provided technical expertise in the assessment of problems reported by national coordinators and additional information sources during the rollover.

Mathematical Modeling of Materials Science Applications

The Mathematical and Computational Sciences Division, together with scientists in the Materials Science and Engineering Laboratory, are collaborating with researchers in England, France, and Belgium on the mathematical modeling of solidification and other applications of phase transformations in materials science. The work is partially funded by the Microgravity Research Division of NASA and has also been supported by a NATO Collaborative Research Grant. The work includes studies of diffuse interface models of solidification with the Industrial Applied Mathematics Group at Southampton University, United Kingdom, studies of interface demarcation by Peltier pulsing with the Universite d'Aix-Marseille III in Marseille, France, and studies of thermal diffusion during directional solidification with the Universite Libre de Bruxelles in Brussels, Belgium.

Protocol Modeling of Bluetooth™ Specification

David Cypher, Advanced Network Technologies Division, collaborates on the development of the Specification and Description Language (SDL) models for the Bluetooth™ specification. When the Bluetooth™ Special Interest Group (SIG) submitted its specification for consideration as a standard to the IEEE 802.15, Cypher, with help from guest scientist Yunming Song, quickly developed SDL models. These protocol models clearly showed the problems that need to be addressed in the Bluetooth™ specification before the IEEE 802 can adopt it as a standard. The Bluetooth™ SIG (www.bluetooth.com) is an international consortium developing specifications for Pico-Cellular network systems. The specification addresses wireless, network, self-discovery, and application areas.

Text Retrieval

ITL's Text REtrieval Conference (TREC) series, which focuses on the creation, administration, and analysis of large text collections to support research in information retrieval, has inspired similar evaluation efforts in France (the Amaryllis program) and Japan (at the National Institute of Informatics, formerly the National Center for Science Information Systems). These groups have cited TREC as their model and have asked NIST for guidance and advice. In September 2000, the first Cross-Language Evaluation Forum (CLEF) was held in Lisbon, Portugal. The forum is a cross-language retrieval evaluation activity for European languages that began as a TREC "track" and is now coordinated in Europe in collaboration with NIST. Donna Harman is the ITL contact.

STAFF RECOGNITION

EXTERNAL STAFF RECOGNITION

Ronald F. Boisvert, Mathematical and Computational Sciences Division, received the 1999 Outstanding Contribution Award by the Association for Computing Machinery (ACM). The award cited "his leadership and innovation as Editor-in-Chief of the Transactions on Mathematical Software and his exceptional contributions to the ACM Digital Library project."



Ronald F. Boisvert

Gary Fisher, Software Diagnostics and Conformance Testing Division, was recognized by Government Computer News for outstanding contributions in promoting information technology (IT) in DoC. Fisher was the Y2K standards and testing expert for NIST and DoC.



Gary Fisher

Fern Y. Hunt, Mathematical and Computational Sciences Division, received the prestigious Arthur S. Flemming Award administered by George Washington University and Government Executive Magazine. Hunt was recognized for a sustained record of fundamental contributions to probability and stochastic modeling, mathematical biology, computational geometry, nonlinear dynamics, computer graphics, and parallel computing.



Fern Y. Hunt

Stephen Langer, Mathematical and Computational Sciences Division, and three NIST colleagues received Industry Week's 1999 Technology of the Year Award for the development of OOF. OOF is an object-oriented finite-element system for the modeling of real material microstructures.



Stephen Langer

Nien-Fan Zhang, Statistical Engineering Division, joined five NIST colleagues as winners of the prestigious 2000 Federal Laboratory Consortium (FLC) Award for Excellence in Technology Transfer for their work on the SEM monitor.



Nien-Fan Zhang

DEPARTMENT OF COMMERCE (DoC) 2000 MEDAL AWARDS

Victor R. McCrary and John Roberts, High Performance Systems and Services Division, received the Gold Medal Award for Leadership for proactively facilitating and developing the first global industry standard for electronic books.



Victor R. McCrary

Kendra Cole, Office of the Director, was part of a NIST Chief Financial Office group selected to receive the Silver Medal Award for Exceptional Service for their efforts in managing and preparing the FY94-FY99 financial statements for NIST and other DoC agencies.



Kendra Cole

Darren L. Smith, Distributed Computing and Information Services Division, was awarded a Silver Medal Award for Scientific/Engineering Achievement for his contributions to the Boulder Research and Administrative Network (BRAN). BRAN is an 11-mile fiber optic network completed this year as a collaborative effort among the NIST Boulder Laboratories, the City of Boulder, the National Center for Atmospheric Research (NCAR), and the University of Colorado.



John Roberts

Nien-Fan Zhang, Statistical Engineering Division, and a NIST colleague in the Manufacturing Engineering Laboratory received a 1999 Silver Medal Award for Scientific/Engineering Achievement for the invention and development of a scanning electron microscope (SEM) image sharpness monitor that serves as an effective solution to the costly industrial metrology problem.



Darren L. Smith



Nien-Fan Zhang



W. George, J. Devaney, S. Satterfield, P. Ketcham, T. Griffin (starting back, left to right)

Judith Devaney, Peter Ketcham, Steven Satterfield, William George, and Terence Griffin, High Performance Systems and Services Division, received the Bronze Medal Award for Scientific/Engineering Achievement in collaboration on Bose-Einstein condensate modeling and visualization.

Jonathan Fiscus, William Fisher, John Garofolo, Alvin Martin, David Pallett, and Mark Przybocki, Information Access Division, received the Bronze Medal Award for Scientific/Engineering Achievement for leadership provided to the spoken language research community in the development and implementation of benchmark test protocols for large vocabulary speech recognition and speaker recognition technologies.

M. Przybocki, J. Fiscus, J. Garofolo, A. Martin, W. Fisher, D. Pallett (left to right)

NIST AWARDS

Stephen Langer, Mathematical and Computational Sciences Division, and two NIST colleagues in the Materials Science and Engineering Laboratory received the Jacob Rabinow Applied Research Award for outstanding achievement in the advancement of computational tools for simulating materials with complex microstructure.

Fernando Podio, High Performance Systems and Services Division, received the William P. Slichter Award for establishing NIST as a leader in the facilitation and development of open software standards and interoperability for commercial biometric systems.



Fernando Podio



SERVICE TO NIST

In FY 2000, ITL supported the NIST staff, clients, and collaborators through a wide range of technical expertise and consulting services. In addition to computing support, we cooperated in many joint projects with the other NIST laboratories. Finally, we sponsored many conferences, workshops, seminars, and training opportunities for the ITL technical staff and our NIST colleagues.

COMPUTING SUPPORT TO THE NIST STAFF

We provided our NIST customers with an array of scientific and administrative computing services, including the following:

- a state-of-the-art scientific computing capability, which encompasses shared-memory parallel systems including three powerful SGI™ Origin™ 2000 servers, each with 32 processors and 32 Gigabytes of memory, and one 8 CPU Origin™ 2000. Distributed-memory parallel computing is handled by an IBM® SP2® with 80 processors, including some specialized for running molecular packages such as Gaussian and GAMESS. There is also a PC cluster for distributed-memory parallel jobs and an IBM® workstation cluster for applications. Specialized visualization hardware (including stereo) enables complex rendering tasks. Parallel consulting services support the needs of the NIST scientific staff in the use of this specialized equipment;
- advanced prototypes, large-scale testbeds, and reliable systems as part of the continuous improvement in scope and quality of service;
- enhanced computer security services that provide a safe and secure computing environment at NIST;
- a robust distributed heterogeneous environment with support for desktop systems and workstations, network capabilities, information services, and access to external and mobile users;
- common computing environments, information access tools, software development tools, and specialized applications software, including consulting and training that support the use of a substantial collection of popular software packages;



J. Matusiewicz, J. Gift, and G. Richter monitor NIST firewall operations.

- site-wide hardware maintenance for standardized desktop systems and workstations and site-wide software licensing;
- maintenance and repositories for standardized platforms and applications; and
- reliable and secure networking and telecommunications services throughout NIST.

FOCUSED SCIENTIFIC AND TECHNICAL COLLABORATION WITH OTHER NIST LABORATORIES

ITL's mathematicians, statisticians, and computer scientists work closely with scientists and engineers throughout NIST to ensure that the best techniques, methods, and software are applied to problems critical to the mission of the agency. This work ranges from short-term consultations to long-term collaborations. Some examples of collaborative work follow. ITL researchers are

- working with colleagues in Chemical Science and Technology Laboratory (CSTL) to develop more accurate methods for estimating spectra.

- working with a colleague in the Materials Science and Engineering Laboratory (MSEL) in parallelizing X-ray absorption spectroscopy (XAS) code. This resulted in gaining a factor of 50 speedup.

- applying triangulated irregular networks to create terrain models from lidar scanning data of construction sites. This work is helping Building and Fire Research Laboratory (BFRL) engineers to develop techniques for the automated assessment of construction progress.

- using techniques of computational geometry to aid in the processing of images from combinatorial experiments on thin polymer films. This will help scientists from the Materials Science and Engineering Laboratory (MSEL) to extract essential data from the massive amounts of data now being generated using new experimental procedures.

- collaborating with the Chemical Science and Technology Laboratory (CSTL) in applying blind deconvolution techniques to characterize point-spread functions in several types of microprobes. These techniques can be used to improve the quality of micrographs and X-ray maps, and also have applications to image compression and medical image deblurring.

- working with colleagues in the Electronics and Electrical Engineering Laboratory (EEEL) on the modeling of optical materials and components of interest in the telecommunications industry. The development of rigorous models and reliable solution algorithms for the simulation of photonic crystals, currently under development as a new switching technology, is in process.

- collaborating with the Manufacturing Engineering Laboratory (MEL) and the Physics Laboratory (PL) in the study of high-speed machining processes, with the goals of extending tool life, improving the surface finish of machined parts, and enabling the machining of parts that are currently manufactured by other means.

- collaborating with colleagues in the Materials Science and Engineering Laboratory (MSEL) on the development of models of interfacial properties in multiphase systems. These models are useful in developing computational techniques that are employed to study instabilities that arise during materials processing.

- developing software to analyze, visualize and compare DNA sequences and protein sequences. This is being done in collaboration with the Chemical Science and Technology Laboratory's Bioinformatics Software Resource.

S. Sell and D. Kim make final configuration adjustments to the upgraded data communications systems in the Physics Building.



**SELECTED CONFERENCES, WORKSHOPS,
AND TRAINING COURSES**

(sponsored, co-sponsored, or hosted by ITL)

13th Annual Federal Information Systems Security Educators'
Association (FISSEA) Conference

22nd National Information Systems Security Conference (NISSC)

2000 NIST Speaker Recognition Evaluation Workshop

Advanced Network Technologies Division Seminars

BioAPI Users' and Developers' Workshop

Biometric Consortium 2000 Conference

DASE Symposium 2000

Digital Library of Mathematical Functions Seminar Series

DVD '99: Standards, Applications, and Technology Workshop

Eighth Text REtrieval Conference (TREC-8)

Electronic Book 2000: Changing the Fundamentals of Reading

Electronic Documents Conference

First International Common Criteria Conference

Good Guys Guide to Network Security Vulnerability and
Penetration Testing

High Performance Systems and Services Division Seminar Series

Information Technology Laboratory Seminar Series

Key Management Standard (KMS) Workshop

Mathematical and Computational Sciences Division Colloquia
and Seminars

National Information Assurance Partnership (NIAP) Training
Courses

Pervasive Computing 2000

Statistical Engineering Division Training Courses

Third Advanced Encryption Standard (AES3) Candidate Conference

WDM-SA'99, Wavelength Division Multiplexing-Systems
and Applications

ITL publishes a variety of Federal Information Processing Standards (FIPS), guidelines, newsletters, bulletins, and documents online. The Web site is <http://www.itl.nist.gov/itl-publications.html>. A link to information about FY 2000 ITL research papers and other publications can be found at this Web site.

NOTE:

Windows NT® and Windows® 2000 are registered trademarks of Microsoft Corporation in the United States and/or other countries. SGI™, Origin™ 2000, and OpenGL® are trademarks or registered trademarks of Silicon Graphics, Inc. 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.

For more information, 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

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.*

