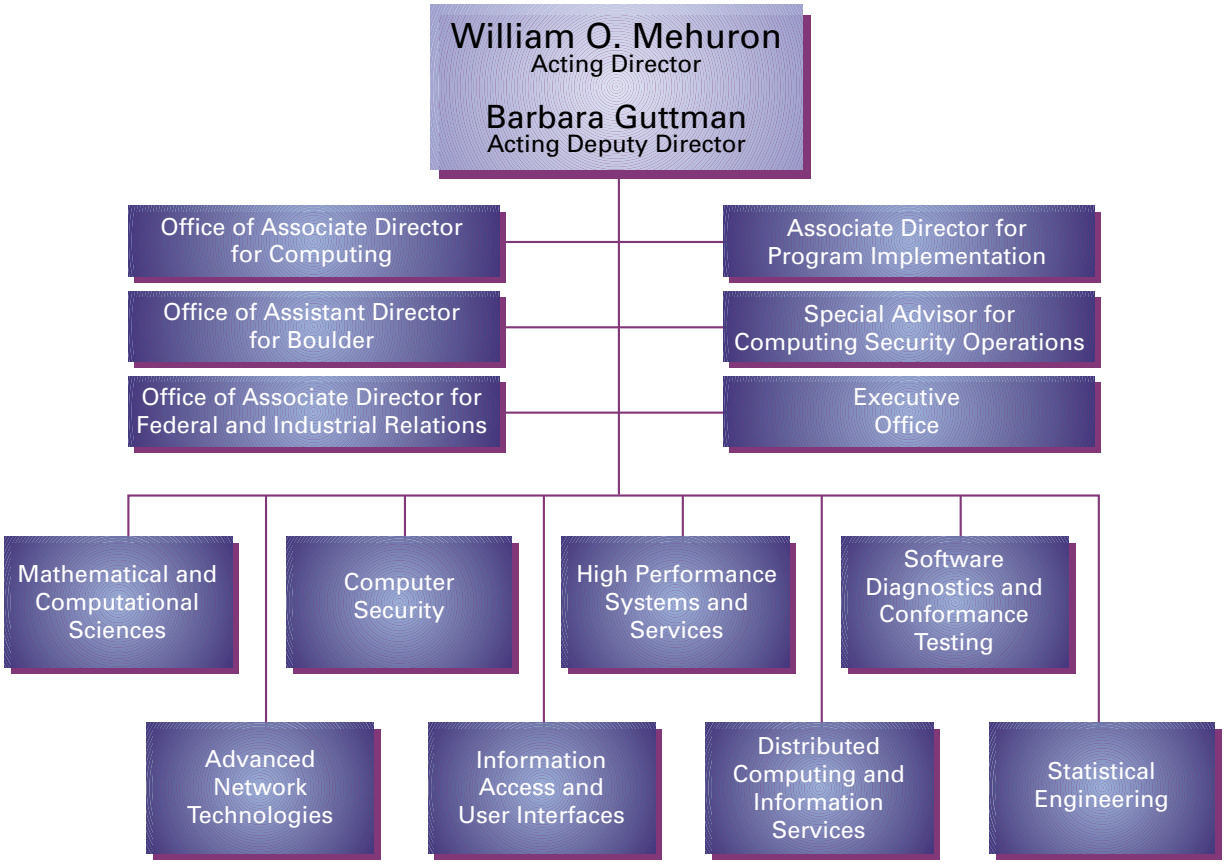
1999

ITL Technical Accomplishments

NIST

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards and Technology
Information Technology Laboratory
NISTIR 6365

Information Technology Laboratory



NISTIR 6365
October 1999

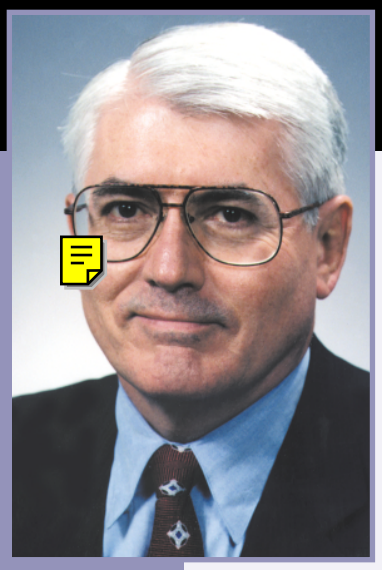
U.S. DEPARTMENT OF COMMERCE
William M. Daley, Secretary

Technology Administration
Gary R.Bachula
Acting Under Secretary for Technology

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

CONTENTS

Director's Foreword 1
ITL at a Glance 3
Technical Accomplishments 6
Industry Interactions 30
International Activities 37
Staff Recognition 40
Service to NIST 42



Director's Foreword

September 30, 1999

Director's Foreword

The Information Technology Laboratory (ITL) is one of the Measurement and Standards Laboratories of the National Institute of Standards and Technology (NIST). ITL's mission is to strengthen the U.S. economy and improve the quality of life by working with industry to develop and apply technology, measurements, and standards for information technology. The laboratory carries out this 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 needed by U.S. industry to produce information technology systems that are usable, secure, scalable, and interoperable. During the past year, ITL was active in the four components of its role, i.e., research, measurement, standards, and service.

We focus on numerous projects that directly affect information technology and its many applications. The most visible is the Advanced Encryption Standard (AES), which will provide a worldwide replacement for the Data Encryption Standard (DES). ITL is conducting an international competition for an AES and recently announced the five finalist candidates. Following a second extensive review and comment period, we plan to select one or more of the finalist AES algorithms and propose it as a Federal Information Processing Standard (FIPS). We participate in a variety of industry consortia and groups; these activities have been an especially effective way to influence industry at an early stage in the evolution of particular technical fields. Examples include:

- biometrics - sponsored a workshop resulting in initial development of an industry specification defining a standard data format for interoperability of biometric devices;

- e-book - worked with industry to develop an interoperable standard for content and completed work on a prototype Braille reader;

- Java Real-time - supported industry in its efforts to develop a real-time Java specification by providing a neutral analysis for specification debates;

- Java Numerics - released a revised version of SciMark, a Web-based benchmark for scientific computing in Java;

- National Information Assurance Partnership (NIAP) - sponsored with industry a healthcare security forum for development of Common Criteria-based protection profiles and tests;

- smart cards - worked with industry on the interoperability and development of standards for smart cards and biometrics;

- speech corpora and testing - conducted initial comprehensive broadcast news tests (word error rates, information extraction, and topic detection and tracking); and

- wireless - developed a testbed for evaluating the performance of various technologies proposed for future generation wireless communication systems.

We identified several new initiatives. The largest of these new initiatives is the laboratory-wide pervasive computing focus. ITL serves as an impartial developer of measurements, testing methods, and standards, and focuses on both short-term and long-term needs in pervasive computing. Among the long-term needs are rich, natural forms of human-computer interaction, such as speech and visual recognition and tracking, sophisticated information access from multimedia databases, extensive information presentation capabilities, collaborative working environments, dynamic networking, security, and reliability.

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. Specifically, 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.

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

ITL at a Glance

***William O. Mehuron**,* Acting Director

Barbara Guttman, Acting Deputy Director

R.J. (Jerry) Linn, Associate Director for Program Implementation

Fred Johnson, Associate Director for Computing

David Kahaner, Associate Director for Federal and Industrial Relations

Paul D. Domich, Assistant Director for Boulder

Kendra Cole, Senior Management Advisor

Robert Raybold, Special Advisor for Computing Security Operations

Ronald Boisvert, Chief of Mathematical and Computational Sciences Division

Kevin Mills, Chief of Advanced Network Technologies Division

Miles Smid, Acting Chief of Computer Security Division

Martin Herman, Chief of Information Access and User Interfaces Division

Dean Collins, 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

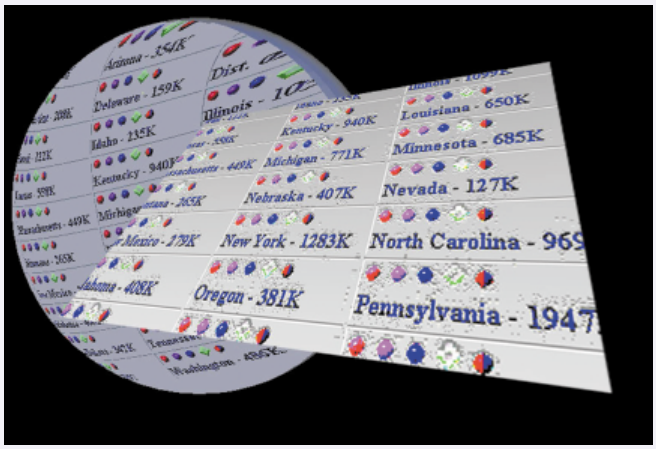
Keith Eberhardt, Acting Chief of Statistical Engineering Division

ITL Mission

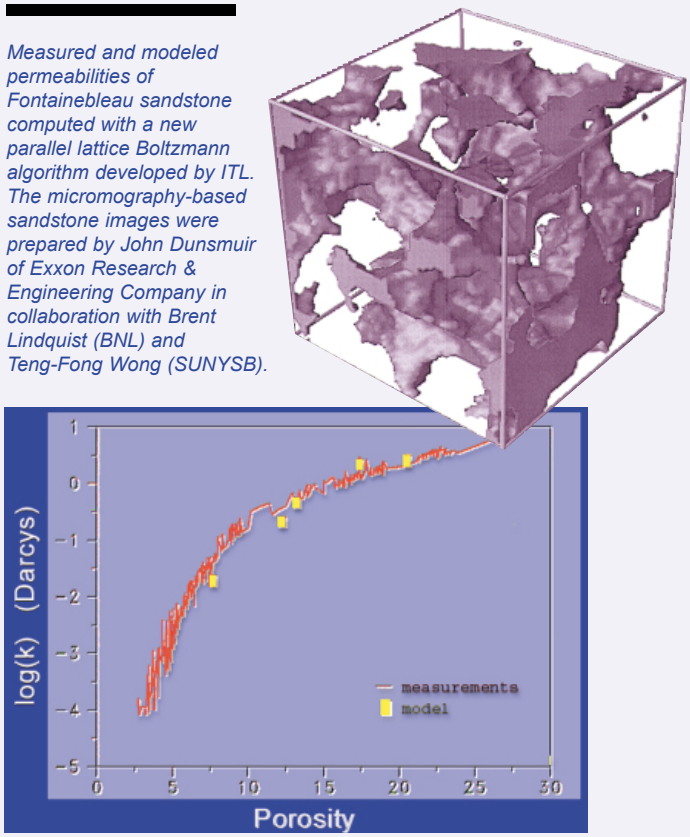
Strengthen the U.S. economy and improve the quality of life by working with industry to develop and apply technology, measurements, and standards for information technology.

In support of its mission, ITL provides

- technical leadership and collaborative research in critical infrastructure technologies that promote better development and the use of information technology, and
- high-quality services and supporting infrastructure to help the NIST staff, its collaborators, and its clients address the measurement and standards needs of many industry sectors.



Excerpt from Web page for FIPS 55 - Place Codes - that provides multiple methods for accessing ZIP codes.



Measured and modeled permeabilities of Fontainebleau sandstone computed with a new parallel lattice Boltzmann algorithm developed by ITL. The micromography-based sandstone images were prepared by John Dunsmuir of Exxon Research & Engineering Company in collaboration with Brent Lindquist (BNL) and Teng-Fong Wong (SUNYSB).

ITL Customers

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

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 476 (includes part-time), supplemented by 109 guest scientists and faculty members (as of September 25, 1999)
- total fiscal year 1999 budget of $74.2M, 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 U.S. industry. The division focuses on the development and analysis of theoretical descriptions of phenomena (mathematical modeling); the design and analysis of the requisite computational methods and experiments; the transformation of these methods into efficient numerical algorithms for high performance computers; the implementation of these methods in high-quality mathematical software; and the distribution of this software to NIST and industry partners.
- The Advanced Network Technologies Division enables the development and deployment of next-generation networking technologies for the transmission of multimedia data streams to enable heterogeneous, collaborative computing. The division collaborates as a partner with appropriate industry groups, rather than with specific vendors, in order to foster the widest possible interoperability among products and services within the communications and computer industry. By focusing on enabling technologies, such as protocols, data formats, and algorithms, ITL delivers the widest possible benefit to the industry.
- The Computer Security Division provides guidance and technical assistance to government and industry in the

protection of unclassified automated information systems. With the growth of electronic commerce and the increased use of distributed systems linked by networks, the need to ensure the security of data and the privacy of information becomes critical.

- The Information Access and User Interfaces 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 the digitization and representation of multimedia data and the use of spoken and written natural language and visual interactive modalities for search and presentation of that information.

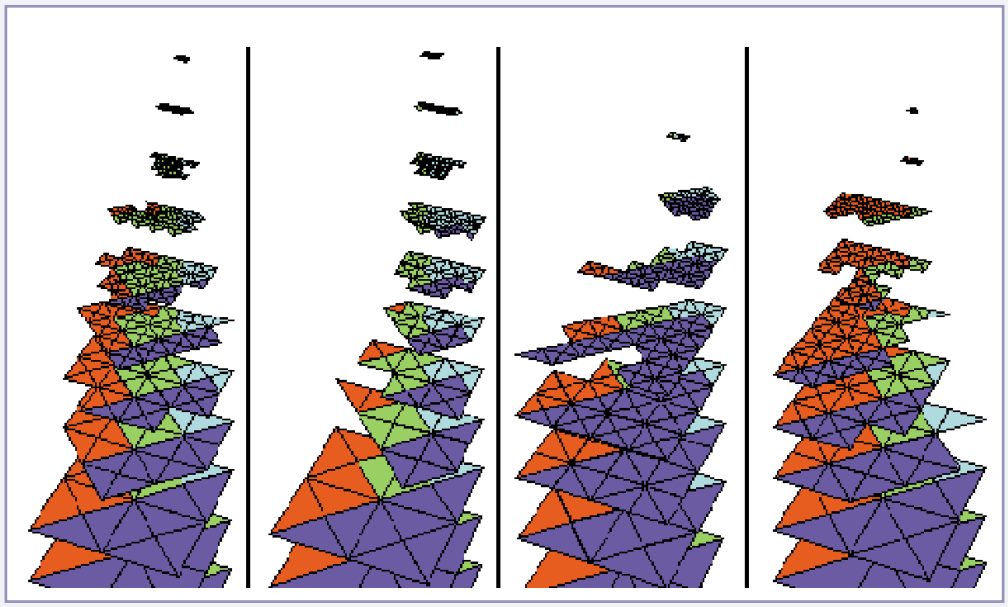
- The High Performance Systems and Services Division enables the effective application of high performance computing and communications systems (HPCC) in support of NIST and its interactions with industry, academia, the federal government, and the public. The division conducts research, development, and evaluation of innovative measurement and test methods, system architectures, and software technologies for improved scalability, functionality, flexibility, reliability, and economy of HPCC. It also provides and manages state-of-the-art facilities that integrate and support an enterprise-wide heterogeneous information technology environment for NIST.

- 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, especially at the early development stage of standards.

- The Statistical Engineering Division advances scientific and industrial research by applying statistical methods to the collection and analysis of data critical to NIST scientists and collaborative partners in industry. Applying statistical tools and methods to NIST research and development programs, division statisticians provide expertise in the development of modeling techniques and analysis relevant to measurement science and technology.

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



This figure uses the f90gl interface to OpenGL graphics to illustrate the grid used to solve a partial differential equation in parallel using an adaptive multilevel grid. Each panel shows the grid on one processor, with the colors indicating which processor is the "owner" of the triangles. The grids have been separated by refinement level to show the multigrid sequence.

Mathematical and Computational Sciences Division Projects

Digital Library of Mathematical Functions

ITL is developing an interactive, richly linked, and network-based Digital Library of Mathematical Functions (DLMF), freely accessible on the Web. It will serve as a new standard reference for the special functions of applied mathematics. The DLMF will replace the classic Handbook of Mathematical Functions (NBS Applied Mathematics Series 55, 1964), a highly cited reference work containing formulas, graphs, and tables that characterize the higher functions of applied mathematics, such as Bessel functions, hypergeometric functions, and orthogonal polynomials. These functions are used extensively in mathematical analysis in many fields, and they remain essential tools in modern computational modeling of phenomena in the physical sciences and engineering. The DLMF will also serve as a model for digital libraries in other areas of mathematics. In FY 1999, ITL obtained significant funding for this project from the National Science Foundation, hosted the first editorial board meeting for the project, identified the first set of authors, contracted for chapter outlines, and released a sample chapter. The Web site is http://math.nist.gov/DigitalMathLib/.

I. Beichl explains the dimer-covering problem during a short course on non-numerical algorithms of use in scientific computing. This year Beichl and colleague F. Sullivan of the Center for Computing Sciences published the most accurate approximation yet to the solution of this problem.

Fortran 90 Bindings for OpenGL

The objectives of this project are to specify a complete Fortran 90 binding for OpenGL, develop a portable reference implementation, and work with external groups to have the binding adopted as an industry standard. Last year, the revised bindings, which were adopted as the standard by the OpenGL Architecture Review Board, were implemented as f90gl Version 1.1, which supports most Unix platforms. In FY 1999, the reference implementation was upgraded to provide support for the new features in OpenGL 1.2 and GLUT 3.7, and to support most compilers under Windows. Several software vendors now provide f90gl-based products. The Web site is http://math.nist.gov/f90gl/.

Guide to Available Mathematical Software (GAMS)

The Guide to Available Mathematical Software is an online service that provides access to a wealth of information about mathematical and statistical software available for use in computational science in an easy-to-use format. Data on software available on internal NIST 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 the University of Tennessee and Bell Labs), is provided. This accounts for nearly 10,000 software components from some 100

packages, both proprietary and public domain. In FY 1999, we continued to revise and update the GAMS server and database to provide a useful service to the community. The more than 120,000 users of GAMS during FY 1999 accounted for some five million Web "hits." The Web site is http://math.nist.gov/gams/.

Java Numerics

ITL conducts assessments of Java's potential for numerical computations and coordinates community activities that seek to improve the usability of Java for high performance computing. Two ITL mathematicians co-chair the Numerics Working Group of the Java Grande Forum. In FY 1999, the Working Group developed a report summarizing Java language issues for numerical computing and presenting a variety of recommendations for future language improvements. ITL presented these results at a panel session at the Supercomputing Conference (SC98) in November 1998 and at the ACM Java Grande Conference in June 1999. Several of these recommendations have already been adopted by Sun; others are in progress. We also developed SciMark, a Web-based benchmark for scientific computing in Java. In a joint effort with the MathWorks, Inc., we developed a model public class library for matrix computations called JAMA, and with the University of Maryland, we developed an alternate design suitable for expert-level users, called Jampack. Both are available on the Java Numerics Web site; more than 2,500 copies of JAMA have been downloaded. The Web site is http://math.nist.gov/javanumerics/.

Matrix Market

ITL developed the Matrix Market to provide algorithm and software developers convenient access to standard, industrial-strength test problems for evaluating the performance of sparse matrix algorithms. The Matrix Market Web site provides test matrices, matrix generation software, search tools, visualizations, matrix I/O software, a bibliography of papers that describe matrices in the collection, submission forms, and associated documentation. Since 1996, the Web site has been visited by more than 76,000 external users, handled more than three million Web "hits," and distributed over 13 Gbytes of matrix data, including more than 52,000 individual matrices. In FY 1999, we maintained the Matrix Market Web service for public access and planned for the addition of a substantial new collection of large test matrices next year. The Web site is http://math.nist.gov/MatrixMarket/.

Measurement Science for Optical Reflectance and Scattering

The main objective of this work is to advance the science of measurements of optical reflectance properties of materials. Measurement techniques and mathematical models for quantifying light scattering are being developed to advance the characterization of surface properties and develop the necessary understanding of the interactions between light and materials. The project is a collaboration among four NIST laboratories and several partners from industry and academia. ITL's High Performance Systems and Services Division is also participating. ITL's main contribution has been in techniques for

C. Witzgall, G. Cheok (BFRL), B. Stone (BFRL), and J. Bernal use triangulated irregular networks (piecewise linear functions representing terrain) to develop real-time modeling techniques for construction sites based on data obtained by lidar scanning.

R. Boisvert, R. Pozo, and B. Miller discuss NIST SciMark benchmark results contributed via the Web. SciMark is a component of the Java Numerics work.

the computer graphic rendering of materials. In particular, more physically realistic models for light scattering are being sought. Based on data from physical measurements, such models have the potential to produce photorealistic images. In FY 1999, these techniques have begun to be tested in computer rendering systems in conjunction with colleagues at the University of Oregon and at Silicon Graphics. The Web site is http://math.nist.gov/mcsd/Staff/FHunt/webpar4.html.

Micromagnetic Modeling

In collaboration with NIST's Materials Science and Engineering Laboratory, ITL is developing open-source micromagnetic modeling tools with experimental verification. Such tools serve as well-characterized reference implementations for evaluating commercial and research software. Partners include IBM, Quantum, MIT, and the Universities of New Orleans, Alabama, and Maryland. In FY 1999, ITL unveiled its first two releases of a solver for 2D problems, along with an extensive GUI. Feedback from industrial and academic users was incorporated into the design. An alpha-level 3D solver was first released in September 1999. The 2D solver is described in the NIST technical report Object Oriented Micromagnetic Framework (OOMMF) User's Guide, Version 1.0. The Web site is http://math.nist.gov/oommf/.

OOF: Object Oriented Finite Element Software for Materials Science

This collaboration with NIST's Materials Science and Engineering Laboratory seeks to develop software for simulating properties of real, highly heterogeneous materials. The PPM2OOF system reads a micrograph obtained in the laboratory, identifies its component parts, and allows the user to assign material properties to them. OOF then allows users to perform virtual experiments to determine the macroscopic properties of the sample. The program has evolved in response to user needs, while maintaining the flexibility of the underlying code. FY 1999 saw numerous enhancements and bug fixes. We added adaptive unstructured mesh generation and manipulations, and new image modification tools. Both programs were ported to Sun and DEC Alpha computers, as well as SGI. In November 1998, ITL published The OOF Manual: Version 1.0 as a NIST technical report. The Web site is http://www.ctcms.nist.gov/~wcraig/oof/.

NIST Sparse BLAS

ITL works with the BLAS Technical (BLAST) Forum to develop community standards for core matrix operations. We are leading the effort for sparse matrix kernels, including the development of interface specifications, reference implementations, and a project Web site. In FY 1999, we participated in BLAST Forum meetings throughout the year, hosting the October 1998 session at NIST. A sparse BLAS standard was drafted, reviewed by the committee, and released for public review within the BLAS Standard document, including C and Fortran interface specifications. Due to changes in the proposed standard, a new version of the reference implementation is being developed. The Web site is http://math.nist.gov/spblas/.

Advanced Network Technologies Division Projects

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

As one of the five funded agencies in the Next Generation Internet (NGI) Presidential Initiative, NIST focuses on the metrology for dense WDM and evaluation of wavelength assignment algorithms. In FY 1999, we developed a WDM metrology laboratory testbed to provide a means to characterize tunable WDM network components with regard to system-level performance. We also developed a WDM network-planning tool, MERLiN, with special focus on wavelength assignment, routing, and reconfiguration. We initiated work on support of Quality of Service (QoS) on WDM networks and mapping of QoS parameters from higher protocol layers such as the Internet Protocol.

J. Wen monitors the performance of the Wavelength Division Multiplexing (WDM) network equipment. D. Su (left), E. Hagley, and F. Lapeyrere examine the test results. The WDM equipment was developed for metrology of optical networks.

Characterization of Broadband Wireless Communication Systems

Local Multipoint Distribution Service (LMDS) is a solution for the so-called "last mile problem" for providing broadband access to business and residential users in a wireless fashion. ITL is developing an accurate model for the communication channel encountered in LMDS, as well as a suitable equalization, coding, and modulation scheme for LMDS. This will achieve excellent communication quality, while offering LMDS at a lower cost than competing technologies. In FY 1999, we developed a channel propagation model for LMDS that adequately captures precipitation effects and blockage by tree foliage. We also developed an appropriate coding/modulation scheme for LMDS. NIST's Radio Frequency Technology Division collaborates in this effort.

Future Generation Wireless Communication Systems

This ITL project focuses on the development of future generation wireless communication systems. The objectives are to evaluate the performance of various technologies proposed for future generation wireless communication systems and to develop new, improved techniques and methodologies for such systems. In FY 1999, working closely with Cadence Design Systems, Inc., we completed the development of a testbed for evaluating the performance of the cdma2000 system in a Cadence SPW platform. Once released, this system will benefit many wireless operators and equipment manufacturers, especially smaller companies that lack the resources to carry out expensive and time-consuming field tests.

NIST Net allows controlled, reproducible experiments with QoS-sensitive Internet applications and protocols to study the effect of Internet performance dynamics on adaptive video applications.

Internet Security and IPv6 Technologies

ITL staff 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). In FY 1999, we announced LibcapV6 and test tools and released NIST Cerberus w/ PlutoPlus, version 1.0. We investigated the use of formal modeling techniques in testing IPsec protocols. Finally, we researched issues relevant to the use of IPsec technology in mobile systems and the use of IPsec in IPv6. Our Computer Security Division collaborates on this project. Web sites are http://www.antd.nist.gov/itg/cerberus/cerberus-users.html and http://www.antd.nist.gov/itg/cerberus/ipsec-wit-users.html.

IP Quality of Service

Through consultations with leading Internet technology research and development companies (including Intel and Cisco), ITL identified industry requirements for test methodologies and tools focused on Internet protocol (IP) QoS issues. Our research and development efforts focus on testing tools to support the design and engineering of QoS sensitive/adaptive applications and developing tools to expedite the research, development, and standardization of emerging IETF signaling, routing, and transport protocols specifically designed for real-time traffic. In FY 1999, we used DIPPER to test our NIST Switch and released the initial prototype of NIST Switch and DIPPER, a multiparty distributed test tool that addresses both functional and performance testing of IP QoS protocols. We also analyzed and experimented with integrated routing, label distribution, and signaling protocols to support traffic engineering in MPLS networks.

Mobile Ad Hoc Networks

A MANET is an autonomous collection of mobile users (nodes) that communicate over wireless links. The objectives of this project are to identify and define metrics for assessing the performance of MANET protocols, to evaluate the performance of various protocols, to develop new, improved methodologies for such systems, to determine the scalability of MANET protocols to large-scale networks, and to make significant contributions to the development of national and international standards for such systems. In FY 1999, we organized and ran the DARPA/NIST Network Simulation and Validation Workshop. We also identified and defined meaningful metrics to compare and evaluate the performance of MANET protocols. On this project, ITL works with SAIC, DARPA, NCS, CECOM, IETF, and proposers of MANET protocols from academia and industry.

MPEG and Image Compression Tools

Working with the Society of Motion Picture and Television Engineers (SMPTE), ITL is developing tools, image fidelity metrics, and standard

reference materials to facilitate the development of multimedia applications and standards (MPEG-2 extensions, MPEG-4, MPEG-7, and multimedia indexing). In FY 1999, we transitioned previous work to higher levels of MPEG, emphasizing object composition. We supported the Binary Format for Scenes (BIFS) activities, gathering BIFS-related programs and data for group distribution. We also distributed a splicing program with respect to SMPTE group efforts. Beneficiaries of this work include multimedia content providers and users of video compression tools.

Networking for Pervasive Computing

Information technology companies foresee an increasing market for technology to support mobile workers who collaborate across organizations. The main objectives of this ITL project are to develop test and measurement technology for pico-cellular wireless systems, to develop methods to assess the function and performance of service discovery protocols, to identify needed technical standards for adaptive middleware, and to demonstrate a networking base to support pervasive computing through the integration of pico-cellular wireless technology, service discovery protocols, and adaptive middleware. In FY 1999, we demonstrated the concept of networking for pervasive computing using a combination of Jini, Java, and wireless LAN technology. Two other ITL divisions collaborate in this work, as well as the Bluetooth Special Interest Group, the HomeRF consortium, and the IEEE 802.15 Personal Area Network standards-setting group.

Programmable Network Technologies

ITL staff actively participates in the research and development of advanced, programmable network technologies. Currently, these activities focus on the research and development of adaptive middleware to enable scripting of reconfigurable distributed systems and the development of test and measurement techniques to enable resource control in active networks. In our adaptive middleware project, we designed a scalable, failure-resilient location management system. We designed, developed, and released to the community an initial version (0.1) of AGNI, a middleware framework and toolkit that implements the Mstream abstraction for reconfigurable distributed systems as an extension to TCL. This initial release includes platform support for both Windows NT and Unix. In the active networks project, we focused on research of computational resource measurement techniques for active network environments. Several other NIST divisions and research communities collaborate.

Streaming Synchronized Multimedia

Streaming multimedia from a Web or video server is a new approach to playing audio and video over a network. This technology provides live multi-cast capability and instant replay for archived clips from selected media streams. In FY 1999, we created ACTS (Annotation Collaboration Tool via the Synchronized Multimedia Integration Language [SMIL]), a Java Applet-based SMIL 1.0 (with extension) player for a manufacture welding collaboration application. We created an MPEG-4 software repository Web site for hosting all MPEG-4 players, utilities, and BIFS datasets. We also continued to work on and promote SMIL standards as the Internet multimedia Web content technology.

S. Shah, H. Fang, R. Glenn, and S. Frankel work on the development of test and measurement tools for Next Generation Internet technologies including IP QoS, IPv6, and Internet security protocols.

Computer Security Division Projects

Advanced Encryption Standard

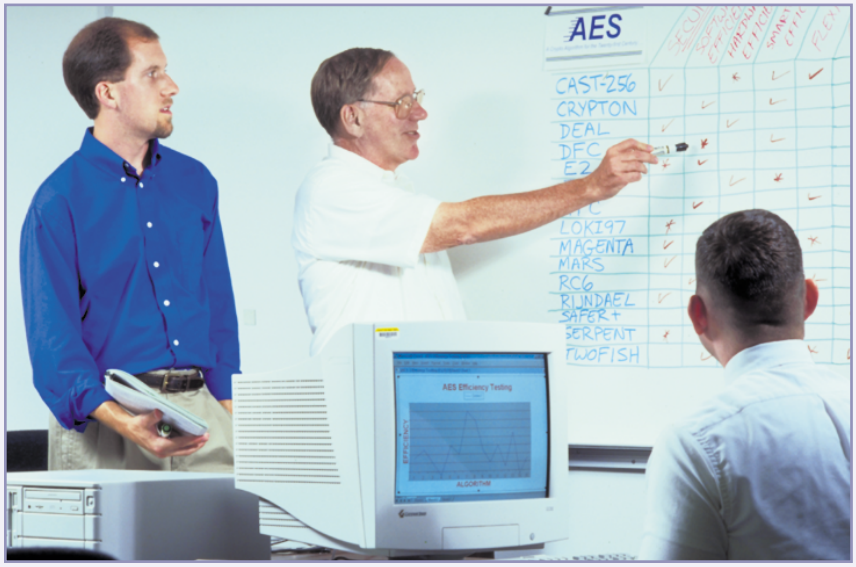
ITL is developing a Federal Information Processing Standard (FIPS) for an Advanced Encryption Standard (AES) that specifies an encryption algorithm(s) capable of protecting sensitive (unclassified) government information well into the 21st century. In FY 1999, we analyzed the comments received from industry, academia, standards bodies, and the public on the 15 initial candidate algorithms. We initiated laboratory-based measurements of the performance of the candidates on the specified AES test evaluation platform. We considered input from the Second AES Candidates Conference, held March 22-23, 1999, in Rome, Italy. Finally, we announced five finalist candidates in August 1999 and initiated a Round 2 review process, which concludes May 15, 2000. The Web site is http://www.nist.gov/aes.

Computer Security Resources Clearinghouse

ITL's Computer Security Resource Clearinghouse (CSRC) provides access to crisis response information as well as information on security-related threats, vulnerabilities, and solutions. Along with references to other computer security programs, 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 1999, we continued to enhance the CSRC by coordinating the site content with the federal Chief Information Officers (CIO) Council Security Committee. The Web site is http://csrc.nist.gov.

Cryptographic Module Validation Program

A joint effort between ITL and the Communications Security Establishment (CSE) of the Government of Canada, the Cryptographic Module Validation Program (CMVP) validates cryptographic modules to Federal Information Processing Standard (FIPS) 140-1, Security Requirements for Cryptographic Modules, and other cryptography-based standards. Results of independent testing performed by accredited laboratories provide this metric. In FY 1999, the program



J. Foti, M. Smid, and E. Roback analyze the cryptographic algorithms under consideration for the Advanced Encryption Standard (AES).

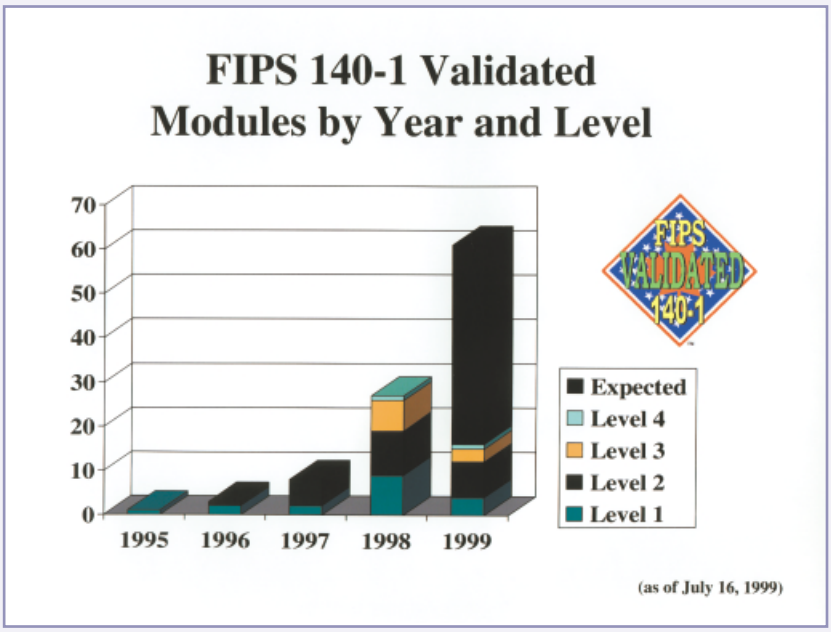
reached a milestone with the validation of more than 60 products, as well as the first validation at Level 4 of FIPS 140-1, the most secure level. Federal agencies, industry, and the public can choose from products on the FIPS 140-1 Validated Products List and have confidence that the products meet the claimed level of security. The Web site is http://csrc.nist.gov/cryptval.

Encryption Key Recovery

ITL supported the Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure, chartered in July 1996 to develop technical requirements for key recovery products. The committee finalized its work in November 1998 and reported its findings to the Secretary of Commerce. As the first step in developing a federal encryption key recovery standard, NIST is seeking industry public comment on the Committee's technical recommendations. In FY 1999, we continued with standard development activities, including developing implementation guidance and a conformance-testing program. The Web site is http://csrc.nist.gov/tacdfipsfkmi/.

GITS Information Technology (IT) Security Training

In 1998, the Government Information Technology Services (GITS) Board gave leadership responsibility of the IT Security Training and Awareness Resource Center to ITL. The project promotes the need for IT security training throughout the government, coordinates the dissemination of laws, policies, procedures, and training materials, and identifies, modifies, and develops standardized training materials for federal agencies. In FY 1999, ITL implemented the underlying technical foundation for the GITS Web site and determined priorities for types of materials, by user role, technology type, and subject matter, to be populated in the repository. Based on these priorities, we collected, modified, and developed materials to fill the repository and will continue this process throughout the life of the project.



FIPS 140-1 Validated Modules by Year and Level

Internet Protocol Security (IPsec) and IPv6

IPsec provides authentication, integrity, and confidentiality services for both the current Internet protocol (IPv4) and for IPv6. The project enables smaller industry vendors to jump-start their entry into IPsec, facilitates and expedites the deployment of IPsec, and promotes IPsec interoperability testing. In FY 1999, ITL contributed to the technical development of the Internet through its participation in the Internet Engineering Task Force (IETF) in the areas of IP security, key management, IPv6, IP integrated services, resource reservation, IP switching, and advanced routing. We developed several specifications for emerging Internet protocols with key industry partners, including Cisco Systems Inc., Bay Networks, IBM T.J. Watson Research Center, the National Security Agency, and Sable Systems. ITL's Cerberus, PlutoPlus, and IPsec-WIT are widely used by industry for interoperability testing and as a reference for commercial IPsec products. The Web site is http://csrc.ncsl.nist.gov/ipsec.

Representatives from five countries signed an Arrangement on the Mutual Recognition of Common Criteria Certificates on October 5, 1998.

Mobile Agent Security

ITL's mobile agent security project develops proof-of-concept prototypes that demonstrate the use of mobile agents for network security testing and network management. We work with industry to develop security standards for mobile agent systems in order to ensure the availability of interoperable and secure agent platforms. Working with the Foundation of Intelligent Physical Agents (FIPA) and a major U.S. IT integrator on mobile agent security in FY 1999, ITL developed a proof-of-concept network security testing and network management tool. We also served as the technical editor to the FIPA security specification and published papers on mobile agent security and the prototype security-testing tool.

National Information Assurance Partnership (NIAP)

NIAP is a NIST/National Security Agency partnership for testing methods and measures to ensure the quality of information security systems. In FY 1999, NIAP developed an evaluation methodology for testing against Common Criteria (CC) specifications. It established a commercial security testing scheme and validation body for National Voluntary Laboratory Accreditation Program (NVLAP) accredited testing laboratories. Protection profiles and tests for telecommunication switches were developed. Finally, NIAP jointly sponsored with industry a healthcare IT security forum for development of CC-based protection profiles and tests. The Web site is http://niap.nist.gov.

Public Key Infrastructure (PKI)

Taking a leadership role in the development of PKI technology, ITL chairs the Technical Working Group of the Federal PKI Steering Committee, which is composed of technology representatives from federal agencies and industry. PKI CRADA partners include AT&T Corporation, CertCo, Certicom Corporation, Cylink Corporation, Digital Signature Trust Company, DynCorp Information & Engineering Technology, Inc., Entrust Technologies, Inc., Frontier Technologies Corporation, ID Certify, GTE, Mastercard International, Microsoft Corporation, Motorola Inc., SPYRUS Inc., VeriSign Inc., and VISA International. In FY 1999, we developed a PKI interoperability testbed, including Secure/Multipurpose Internet Mail Extensions (S/MIME) interoperability testing and a Minimum Interoperability Specification of PKI Components (MISPC) reference implementation. The Web site is http://csrc.nist.gov/pki/.

Random Number Generation (RNG) and Testing

This ITL project defines and programs a set of statistical tests that may be used to verify that the output of a cryptographic RNG appears to match the Bernoulli (fair coin toss) model. The tests are run on various random number generators and the results studied. These tests will be applied to the NIST FIPS-approved random number generators and cryptographic algorithms. NIST plans to make the tests available to the commercial and scientific sectors. In FY 1999, we completed the analysis of tests on RNG algorithms and Advanced Encryption Standard (AES) candidates. In January 1999, ITL submitted the work to the American National Standards Institute (ANSI) for inclusion in the Cryptographic Random Number Generation Standard (ANSI X9.82). ANSI X9.82 will be the standard used by the financial community for random number generation in cryptographic applications. NIST and IBM co-edit the standard.

Information Access and User Interfaces Division Projects

DARPA Intelligent Collaboration and Visualization (IC&V)

At the request of the Evaluation Working Group (EWG) of the DARPA Intelligent Collaboration and Visualization program, ITL supports the development of evaluation methodologies and tools that enable testing and benchmarking of collaborative systems. In FY 1999, we reorganized and updated the EWG Web site and evaluation framework to make it easier for collaborative environment researchers to apply the evaluation methodology. We advised on tool usage for the analysis and visualization of logged data for the manufacturing collaboratory with NIST's Manufacturing Engineering Laboratory. Finally, we constructed a database to collect usage and process information for long-term analysis. The Advanced Network Technologies Division has cooperated in this project. The Web site is http://www.nist.gov/nist-icv.

Face Recognition

The National Institute of Justice requested ITL to develop standards for evaluating digital video face recognition systems, collect a standard database of faces in digital video, and implement and evaluate baseline digital video face recognition algorithms. In FY 1999, we continued to collect data for our digital video database. We also completed computational psychophysics studies in collaboration with the University of Texas at Dallas. ITL developed scoring software for face recognition. The face recognition project will culminate with a video-based human identification conference in 2001. Industry will benefit by having a standard database available for developing and evaluating face recognition algorithms.

Fingerprint / Law Enforcement Standards

In support of the FBI's Integrated Automated Fingerprint Identification System (IAFIS), ITL provides the research and development efforts required for the creation of standards and specifications relating to the quality, format, and transmission of electronic images and related data over a wide area network. In FY 1999, we published a summary report from the workshop held in September 1998 to reevaluate the ANSI/NIST-CSL 1-1993 fingerprint and ANSI/NIST-ITL 1a-1997 mugshot

Researcher C. Martin provides acoustic and video data to the NIST Perceptive Interface experiment in the Smart Spaces Laboratory, while M. Benharrosh and F. Mougin monitor the acquisition and classification components they are developing.

information exchange standards. We initiated the development of a prototype system for a verification and authentication of booking station data by connecting a digital signature to the fingerprint of the booking officer using a smart card. We published a Best Practice Document for the Capture of Mugshots. Finally, we completed the first draft of the updated standard for the interchange of fingerprint and other identification information. The Web site is http://www.nist.gov/itl/div894/894.03/fing.

Java Information Retrieval Framework (JIRF)

ITL is developing (for distribution without restrictions) a portable, extendable, object-oriented framework for information retrieval (IR) along with a basic IR application (indexer and search engine) built on the framework. We based our work on the core of an existing IR framework (FIRE) developed in C++ by researchers at the Union Bank of Switzerland, who gave us permission to distribute freely a Java IR framework based on the FIRE core once its dependencies on a proprietary application development framework (ETOS) and a commercial object database (ObjectStore) had been removed. In FY 1999, we developed an initial implementation of JIRF and sample text retrieval application without support for persistent storage. We then developed a proxy/broker-based persistence mechanism, implemented a file-based instance of it, and began work on scaling the application and framework to support indexing and search of a Text REtrieval Conference (TREC) sized text collection.

Optical Information Processing

The development of better system-level metrology is needed to allow more computer-based methods to be used in the commercial application of optical technology to information processing. As a test case, ITL is designing an optical pattern recognition system to be performed on an input image (at video rates) versus a large reference set, for example 1000 faces, with images of 640 by 480 pixels or larger. We constructed both an optical pattern recognition system and a holographic memory system that we have instrumented and used to address the metrological needs of these applications. In FY 1999, we measured the accuracy of real-time fingerprint correlation and developed standard test measurements for spatial light modulators (SLMs). ITL's High Performance Systems and Services Division and the Mathematical and Computational Sciences Division collaborate on this project.

Spoken Language Technologies Benchmark Tests, Corpora, and Software Tools

ITL advances the development of spoken language technologies by developing test protocols and speech corpora for the training, development, and evaluation of these technologies.

Q. Wang and A. Godil discuss the integration issues for a Virtual Reality Modeling Language (VRML) demonstration for manufacturing applications using a dynamics engine and humanoids.

We continue to advance the state of the art in spoken language technologies by focusing benchmark tests on ever-more-difficult domains such as the recognition of broadcast news recordings in several languages. In FY 1999, we conducted initial comprehensive broadcast news tests, which focused on word error rates, information extraction, and topic detection and tracking. Benchmark test activities were carried out for the following technologies: large vocabulary

continuous speech recognition in several domains and under various speech and channel conditions; conversational telephone continuous speech recognition; multi-lingual continuous speech recognition; broadcast news continuous speech recognition and information extraction; speaker recognition; speech understanding; and spoken document retrieval. NIST spoken language software tools are available at http://www.nist.gov/speech/software.htm.

Text REtrieval Conference (TREC)

Our TREC project encourages research in text retrieval based on large-scale test collections and increases the availability of appropriate evaluation techniques for use by industry and academia, including development of new evaluation techniques more applicable to current systems. At TREC-7 on November 9-11, 1998, 56 groups including representatives from 13 different countries and 19 companies participated. Of special interest was the cross-language track, where groups retrieved English, German, French, or Italian documents using questions in a single language. In FY 1999, we also designed and implemented testing scenarios for performance of Web-based search engines (in collaboration with others) and performed a dry run of a question-answering task. The Web site is http://trec.nist.gov.

Usability Engineering and WebMetrics

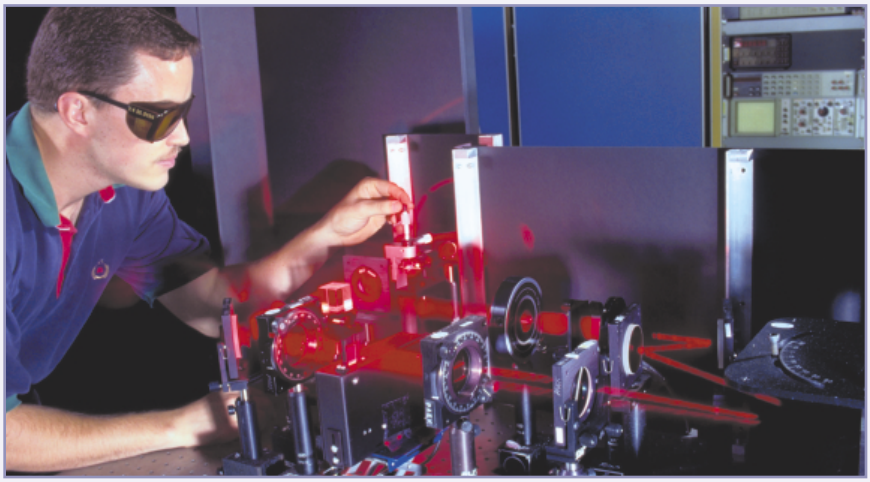
This ITL project promotes the incorporation of usability into software products as a normal part of design and development. In FY 1999, we refined Web usability tools based on feedback collected from our WebMetrics Web site. We released a user path visualization tool (VISVIP). We developed cultural assessment and site branding tools. We developed a common software usability report format, a white paper, and Industry Usability Reporting Project (IUSR) Web sites (public and members only) and began IUSR pilot studies to validate the reporting format with the third industry usability workshop. Finally, we participated in government committees to implement new accessibility federal regulations. The Web sites are http://www.nist.gov/webmetrics and http://www.nist.gov/iusr.

Visualization and Virtual Reality for Manufacturing

With NIST's Manufacturing Engineering Laboratory, ITL is investigating the use of advanced visualization environments to enable more intuitive interfaces to manufacturing data. In FY 1999, we provided a set of Virtual Reality Modeling Language (VRML) integration guidelines based on our prototypes and translation tools. We extended the use of virtual worlds to collaborative interactions in the context of multi-user environments. VRML is being used to visualize distributed collaborative spaces aimed at facilitating design and engineering analyses for remote participants. In addition, participants not able to attend various meeting and presentations will be able to review presentations via a meeting summarization system created using off-the-shelf components. The Web site is http://ovrt.nist.gov.

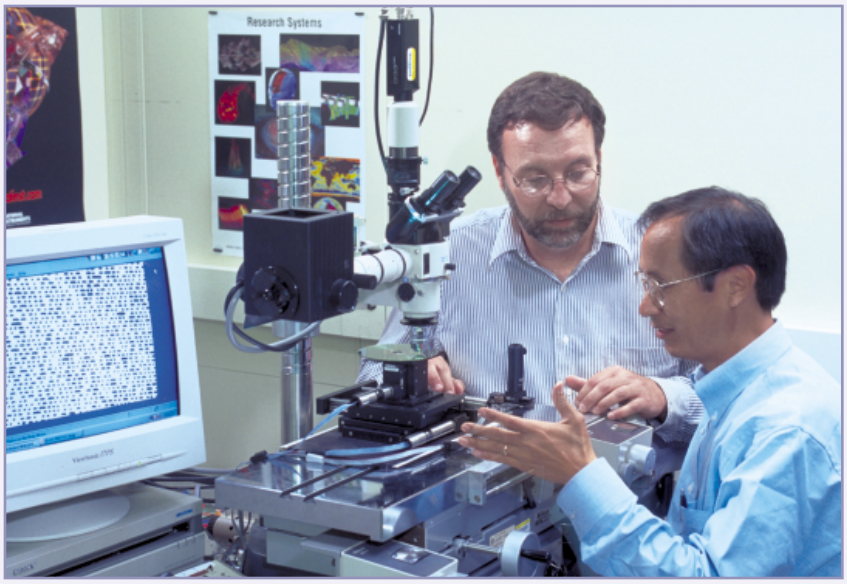
Visualization for Access to Complex Documents

ITL is demonstrating the use of three-dimensional visualization as a valuable interactive medium between the user and a retrieved set of documents. In FY 1999, we completed a study of a visualization prototype (NIRVE) and submitted papers for publication. We also prototyped the visualization of documents on a large-screen display and created a test scenario for collaborative training visualization. The Web site is http://www.nist.gov/nirve.



C. Watson shows the Optical Pattern Recognition System working using fingerprints.

High Performance Systems and Services Division Projects



F. Byers and X. Tang test reliability of a digital versatile disc (DVD). Digital information stored on the DVD can be seen on the screen through a microscope.

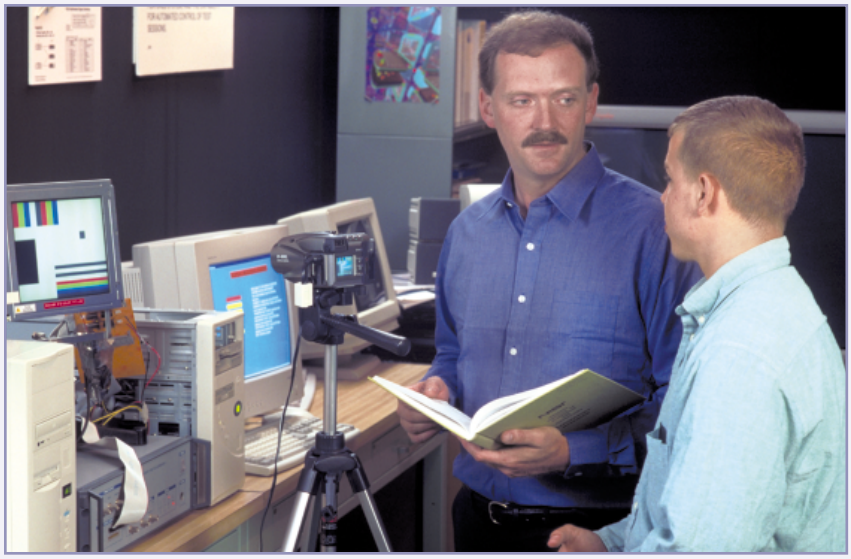
Advanced Digital Data Storage: Metrology and Interoperability for Optical Disc Storage

ITL's Digital Versatile Disc (DVD) research explores the reliability and suitability aspects of DVD-RAM media as a replacement for current magnetic media for computer data mass storage. DVD-RAM is also being investigated as a storage media for high-definition television (HDTV), providing complementary support of the Digital Television Application Software Environment (DASE) HDTV project. The project is developing standards and test methods for optical disc reliability and interoperability for writable optical disc storage platforms and evaluating DVD-RAM media as a future storage media for high performance computing. In FY 1999, we completed the image processing of optical disc surface features and initiated the development of an advanced storage measurement system. In support of this work, ITL co-sponsored the SPIE Optical Disk Conference in July 1999 and the DVD '99 Industry Workshop. By working with the DVD industry, ITL provides vendor-neutral research on the performance and ruggedness of DVD-RAM media for archival applications. The interoperability of DVD-RAM media and media interchange tests increase the market success and user confidence in this new generation of products. The Web site is http://www.nist.gov/itl/div895/isis/projects/.

Biometrics Technologies and Smart Cards: R&D, Measurements and Standards

ITL is working with industry on the interoperability and development of standards for smart cards and biometrics. Commercial business drivers for these technologies are rapidly increasing. As a neutral partner uniquely qualified to help U.S. industry in the development of measurement and standards, ITL seeks to achieve interoperability for biometric devices and smart cards through research and development coupled with the facilitation of industry standards. ITL's Information Access and User Interfaces Division collaborates in the research effort. In FY 1999, we established a

testing and interoperability laboratory for biometric devices/subsystems and smart cards. We set up interoperability tests and initiated testing protocols. We opened our NIST Biometrics laboratory to industry users. As co-chair of the U.S. Biometric Consortium (BC), we co-sponsored the BC Fall '99 Conference with the National Security Agency. The Web site is http://www.nist.gov/itl/div895/isis/projects/.



J. Roberts discusses display stimuli with J. Ward.

Digital TV Application Software Environment (DASE)

ITL works with the Digital TV Applications Software Environment (DASE) specialist group (T3/S17). As part of the Advanced Television Systems Committee (ATSC), the group is developing a standard DASE Application Programming Interface (API) so that digital TV content providers can build an application, using these APIs, which will run on any conforming manufacturer's equipment (the TV set-top unit or STU). The specialist group requested ITL to develop a reference implementation for their API and to support the development of associated conformance tests. Our Software Diagnostics and Conformance Testing Division collaborates in this effort. The NIST reference implementation will serve as the benchmark implementation upon which other implementations can be compared to confirm adherence to the DASE specification. In FY 1999, the T3/S17 DASE committee progressed toward a definitive definition of the API. We worked with committee participants to refine the definition; the document must be finalized before an implementation (our project) can proceed to full effort. Industry partners include Sun, General Instruments, MicroSoft/WebTV, Teralogic, ABC, NBC, Disney, PBS, CBS, Fox, Motorola, Philips, Samsung, Sony, and Panasonic. These companies look to a NIST reference implementation of the DASE specification to assist them in developing interactive digital TV services. The Web site is http://www.nist.gov/itl/div895/cmr.

Electronic Book: Concept Development and Standards

ITL researchers constructed a working prototype electronic book reader, with two screens functioning as two pages, touch screen control, page forward/back, search, bold, underline, font size control, bookmark, annotation, and a preliminary dictionary look-up. In FY 1999, we migrated from a visual basic platform to an HTML platform for our e-Book prototype and completed work on our prototype Braille reader. We also worked with industry to facilitate the development of an interoperable standard for electronic content of electronic books. Through the Open Electronic Book Standards Committee, ITL participated in the development of a draft specification, OEB 1.0. We co-sponsored the Electronic Book '99 Workshop with the National Information Standards Organization (NISO). Industry partners include Softbook, NuvoMedia, Microsoft, Librius, Everybook, Glassbook, Random House, Xerox PARC, McGraw-Hill, Harper-Row, IBM, R.R. Donnelly, Adobe, Scholarly Technology Group - Brown University, Exemplary Technologies, Vadem, Versaware, Nokia, OverDrive Systems, FX Palo Alto Laboratory, GlobalMentor, The Productivity Works, Red Figure, Simon & Schuster, Project Guttenberg, and The DAISY Consortium. The Web site is http://www.nist.gov/itl/div895/isis/projects/.

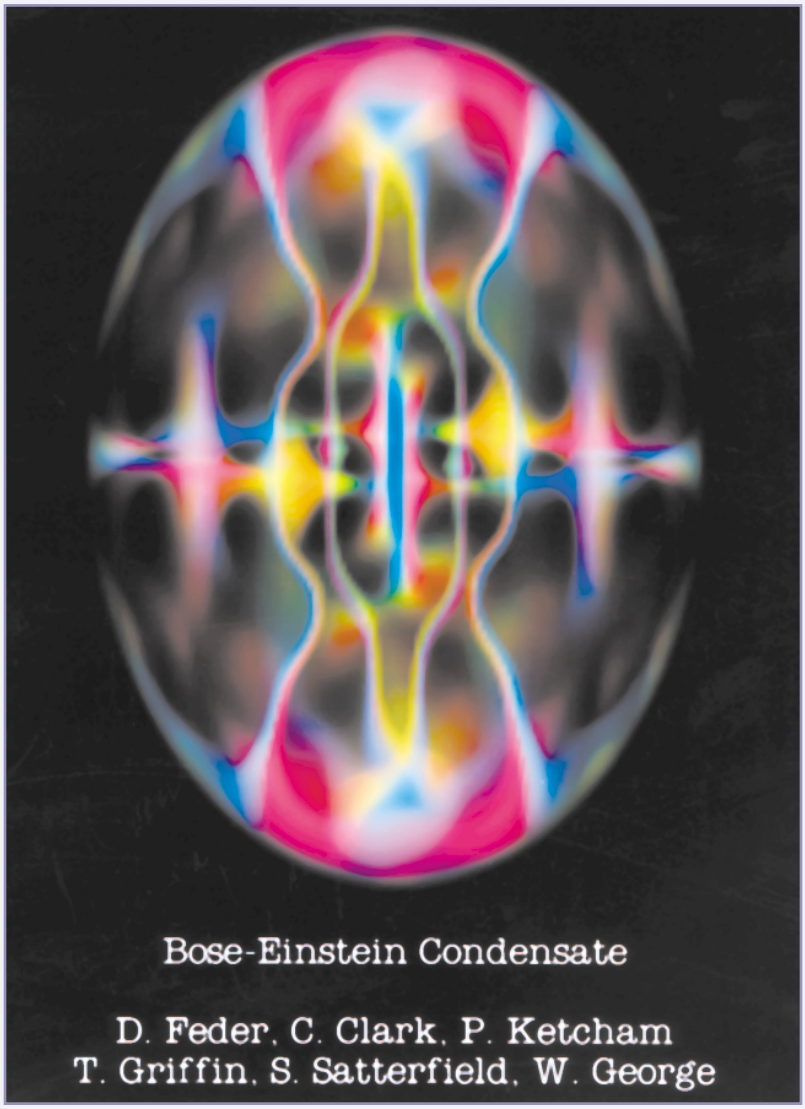
Interoperable Message Passing Interface (IMPI) and Conformance Tester

Working with computer vendors who are designing a standard for interoperability among different MPI implementations, ITL facilitates the effort by convening meetings, writing tests, and providing the IMPI conformance tester. In FY 1999, ITL hosted the seventh and eighth meetings of the vendors who are evolving the standard and released the IMPI draft standard for comments. We completed and released the IMPI conformance tester. Using a novel approach to the tester, we arranged for the testing to be done over the Web using Java. Vendors connect to the ITL IMPI home page, download the tests, and run the tests between ITL and their implementation. Results (pass/fail, details) are immediately available on the Web page. The Web site is http://impi.nist.gov/IMPI.

Performance of Distributed Architectures

This ITL project seeks to determine and enhance the ability of networked system architectures to handle computational demands arising in scientific computing, electronic commerce, and other evolving inter-LAN applications. Some system design studies were made with NIST's Building and Fire Research Laboratory on specialized clusters for advanced modeling, while ITL cooperated with the Physics Laboratory in improving their time distribution schemes. Performance evaluations of PC clusters showed that they provide a significant level of computation power with a very attractive price/performance ratio. As a result, we moved a 333 MHz Pentium II cluster, along with a Fast Ethernet switch, from our research group to ITL's production computing services to join the IBM SP-2 and SGI Origin 2000. A second PC cluster joined the first to check new configurations offline. Our local and GPS time synchronization instrumentation is employed to refine these clusters. Our instrumentation also identifies causes of network variation that limit any time-stamp synchronization scheme limited solely to Internet mechanisms. The Web site is http://www.nist.gov/itl/div895/research/PC_Clusters/sld001.htm.

First renderings of vortices, in a trapped Bose-Einstein Condensate under rotation, produced by a computational model. These results are predictions for the kinds of structures, which are classic manifestations of superfluidity that should appear in an actual experiment.



Distributed Computing and Information Services Division Projects

Commerce Standard Acquisition Reporting System (CSTARS)

This ITL project began when the Department of Commerce (DoC) awarded a contract to CACI for procurement management software. NIST is the pilot agency within DoC for implementation of the COTS CACI/SACONS Procurement Automation System. In FY 1999, the contractor developed a full project plan with an implementation timeline. We reviewed preliminary designs and met with DoC and the contractor. We also visited other government sites where SACONS has been implemented. Upon successful completion of the project implementation at NIST in 2000, other parts of DoC will implement the system, starting with the Office of the Secretary.

Computer Security Initiative

Computer security has become increasingly important to all NIST computer systems, especially for standalone workstations. ITL assists the owners of compromised systems to recover from intrusions and configure their machines so they are as secure as possible. In FY 1999, we created a team to help NIST staff with compromised computers to recover from those compromises. The team has responded to more than 25 incidents. The team also reconfigured more than 10 workstations in NIST's Manufacturing Engineering Laboratory to fix security problems. ITL also developed security checklists for Unix and NT computer systems to assist users in setting up secure systems.

R. Whetstone and S. Jackson of SATO discuss Travel Manager software requirements with R. Desai (left) and J. Luipersbeck (right).

Electronic Mail Enhancement

To improve e-mail service for the NIST staff, ITL is enhancing the NIST electronic mail system. In FY 1999, we tested the operation of an Internet Messaging Applications Protocol (IMAP) server as a replacement for the Post Office Protocol (POP) server that is currently being used on the central NIST server for accessing users' mail. To explore the consequences of implementing an IMAP server, ITL implemented a server with a limited number of users. As experience is gained, modifications to the server will be made to accommodate more users. We also augmented the server's disk storage capabilities.

Enterprise Calendaring System

To upgrade the current NIST enterprise calendaring system that was slow and unreliable, ITL investigated and tested two systems to replace the current system. In FY 1999, we selected CorporateTime as the candidate to be recommended to NIST management because it had an exceptional reputation with current users (determined from visiting or interviewing three sites similar to NIST) and would cause minimal disruption to the existing NIST messaging infrastructure. The procurement of the selected package is in process, and we will transition to the new system in 2000.

ITL Public Web Page Revision

ITL wants to provide the public and NIST staff with a usable and informative Web site. In FY 1999, we collected data on the current Web site, established the audience(s), and solicited ideas from the ITL staff. We worked on various design possibilities, including an ITL logo, the Web site, and other related identity pieces. We incorporated input from the ITL Division Chiefs into our designs and submitted preliminary designs to the ITL Director. We will release the new Web site in 2000.

Migration to Central Webservers

With the implementation of a NIST Firewall, ITL needed to provide a Web and ftp hosting service for all NIST Web pages that need to remain publicly accessible. In FY 1999, we moved all subnets and NIST Laboratory Web pages behind the firewall. 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. A procedure was developed that pushes the publicly accessible files from the NIST private server (not publicly accessible) to the NIST public server at set time intervals. This procedure creates a more secure public server by removing unnecessary accounts.

Paperless Facsimile Service

The goal of this ITL project is to implement a service that would allow any user of a Windows-based PC to send and receive facsimiles directly from their PC. We tested the HylaFax system, which allows any user of a Windows PC to send facsimiles. For receiving facsimiles, we tested a design that involves converting incoming facsimile data to common image file formats, such as TIFF, GIF, and JPEG. Once the image file is created, a Web browser is able to display each image on the addressee's computer. To ensure privacy, a password will be sent to the addressee to enable viewing the image. The image can be printed when the browser has displayed it. This service is ready for extensive testing by users.

PC Support Baldrige Criteria

To provide a framework for performance excellence, ITL applied the Baldrige Criteria to the mission of our PC Support Group. We determined that the most applicable areas to address were training/skills development, employee feedback, and internal procedures.

Jim Porterfield discusses SMIL technology with C. Wines (Public and Business Affairs). The wall is covered with copies of Porterfield's poster creations.

D. Osborne tests software for verifying the ability of PCs to properly process dates after 1999.

PC Support examined the skill level of its employees and future support requirements. By looking at these two areas, we identified future training needs and compiled a training schedule. We surveyed the PC Support group and used the feedback to make needed changes. We also examined internal procedures and rewrote procedures to better reflect workflow processes.

PC Support Managed Desktop

This ITL project utilizes emerging technologies to provide better customer support by managing the customer's desktop. Since many calls to PC Support involve complex problems, it would be valuable if the PC Support staff member could take over control of the customer's PC to correct the problem. This action would save many office visits, increasing the productivity of the PC Support staff while offering the customer faster service. Additionally, other utilities could be used to manage the software on the customer's desktop in order to keep the customer up to date with the latest versions of NIST standard software. Currently in the planning stage, this project will be implemented in 2000.

Travel Manager Upgrade

Since the older version of Travel Manager, version 5.0, used at NIST was not Y2K-compliant, this project provided the NIST staff with Y2K-compliant travel software, which also is more conducive to electronic processing procedures. In FY 1999, we configured Travel Manager for both general administrative and electronic processing functions, assisted the contractor Gelco with data format conversion, and migrated to the new travel server. We also did post-conversion data modification. Finally, we trained NIST staff on the new system, Travel Manager, version 7.1A.

Windows NT Support Initiative

ITL's NT service team provides reliable and timely service to the NIST staff. In FY 1999, the team prepared and implemented a design for a secure computing architecture (a domain) for NT servers for Gaithersburg and Boulder. We managed servers as requested by the NIST Laboratories, consulted with server administrators concerning operational problems, expanded the NIST NT domain, and planned for changes necessitated by the next release of the operating system.

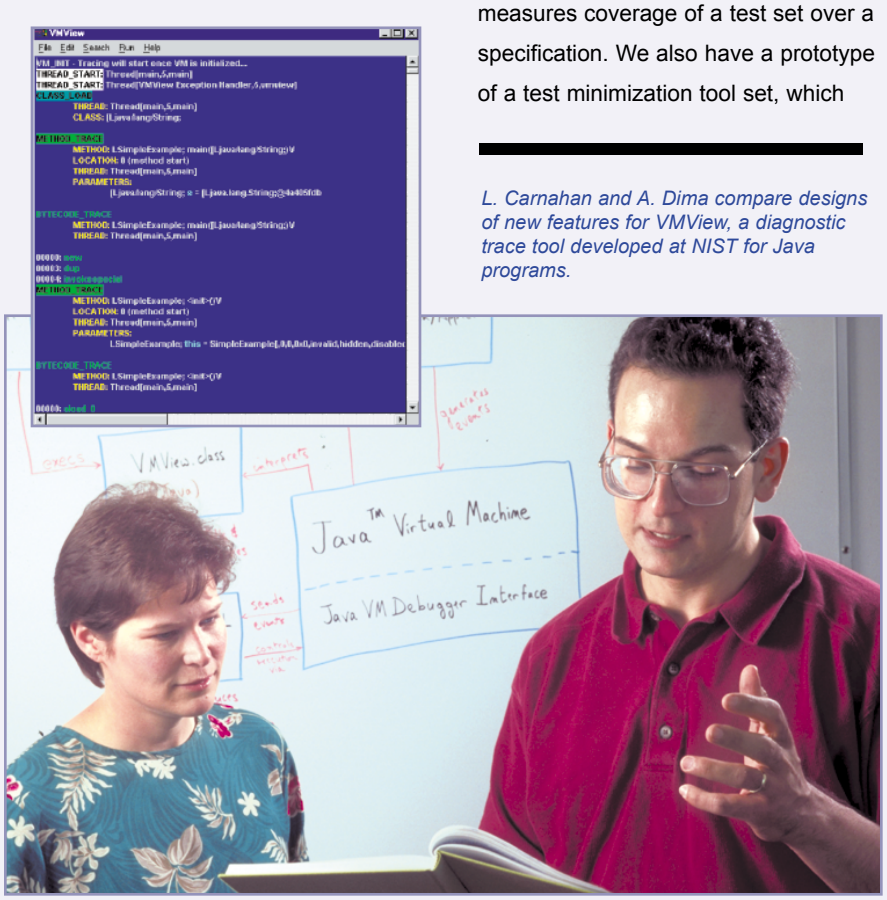
Year 2000 Software / Hardware Remediation

ITL assessed the impact of Y2K on NIST hardware systems and software systems containing dates, making modifications when needed, testing and verifying results, and developing contingency plans. In FY 1999, we completed software renovations of all administrative systems and developed Y2K contingency plans for these systems. We evaluated PC software Y2K remediation packages and completed production of PC Y2K Compliancy Kits, which included a diskette for hardware testing and instructions for checking software and performing updates via the PC Support Web site.

Software Diagnostics and Conformance Testing Division Projects

Automatic Generation of Tests from Formal Specifications

Initiated as a competency effort to improve the state of the art in automated test generation, this ITL project focuses on developing methods to produce software tests, including conformance tests, from formal specifications. These methods promise significantly more economical means for testing software than are currently available. This will reduce time-to-market for companies producing software products. The project will be successful if the benefit derived from producing tests automatically, rather than current methods, exceeds the cost of producing formal specifications. In FY 1999, we developed a prototype test generation tool, which turns a test case into a finite state machine. This prototype is used in a new tool that measures coverage of a test set over a specification. We also have a prototype of a test minimization tool set, which uses the coverage checking tool and a report generator. Transfer of this technology is planned.



L. Carnahan and A. Dima compare designs of new features for VMView, a diagnostic trace tool developed at NIST for Java programs.

Error, Fault, and Failure Data Collection and Analysis

To help industry protect against releasing software systems with faults and to help assess software system quality by providing statistical methods and tools for analysis of software systems, ITL is developing techniques for measuring effectiveness of software methods. Our goal is to provide profiles against which developers can test their software. We are acquiring error, fault, and failure data to develop profiles for industry use and for statistical analysis methods. In FY 1999, we developed and enhanced a prototype public data base capability and analysis tool that will be made available on the Web. We also produced several chapters of a handbook on domain-specific classes of faults. The Web site is http://hissa.nist.gov/project/eff.html.

Java Testing Project

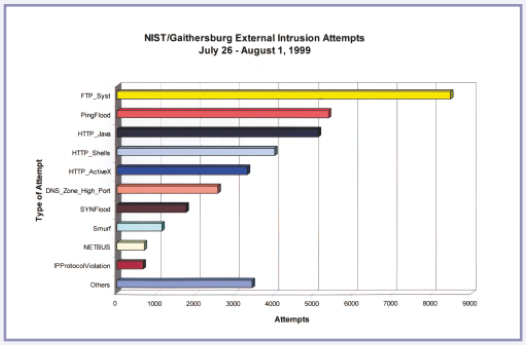
Java has become an integral part of computer technology due to its multi-platform, multi-implementation capabilities. As with any widely used technology, there is the need for conformity assessment methods to

ensure consistency and accurate use of the Java specification now and in the future. In response to industry needs, ITL is focusing its efforts on NIST Test Cases for Java, real-time issues in Java, and VMView. In FY 1999, we implemented new JVMDI functionality into VMView and implemented XML format into VMView trace. We chaired the Java Real-Time Requirements Group, consisting of private sector companies who were interested in a real-time Java specification. We published a NIST technical report on the Requirements for Real-time Extensions to the Java(tm) Platform. We participated in the Real-time Java Expert Group and supported industry in its efforts to develop real-time Java specification by providing neutral analysis for specification debates. The Web site is http://www.nist.gov/java_ca.htm.

Object Oriented Technology and Conformance Testing for Distributed Interactive Learning Systems

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. ITL chairs the EDUCAUSE Instructional Management System (IMS) Conformance Testing Working Group and our researchers are developing conformance tests for the EDUCAUSE IMS Metadata and Packaging standards. In FY 1999, we demonstrated a metadata and repository prototype. We focused on the application and evaluation of prototype metadata repository and tools with distance learning prototype systems and users. The IMS Metadata Specification was finalized. A conformance testing issues document (for IMS Metadata) and a draft security architecture for IMS systems were also issued.

This graph, developed from data provided by the NIST firewall, details both the type and number of external attempts to break into the NIST network during a typical one-week period in which over 36,000 total intrusion attempts were detected. The graph demonstrates the need for the NIST firewall and shows the types of attacks to which user's systems are subjected.



Programs to Evaluate Software Testing Tools and Techniques (PESTTT)

To satisfy an industry need for an unbiased reference suite to evaluate test cases generated by software testing tools, ITL is developing and making available to researchers and tool vendors a diverse and comprehensive suite of program modules. These modules consist of an oracle (specifies expected output for a specified input) and many versions seeded with errors selected from commonly available error taxonomies. In FY 1999, we developed a prototype implementing a subset of features and capabilities, including the design of the application structure, some initial program modules, and a navigation and access tool for the modules. We will post a NIST technical report and an initial suite of C programs on the Web in 2000.

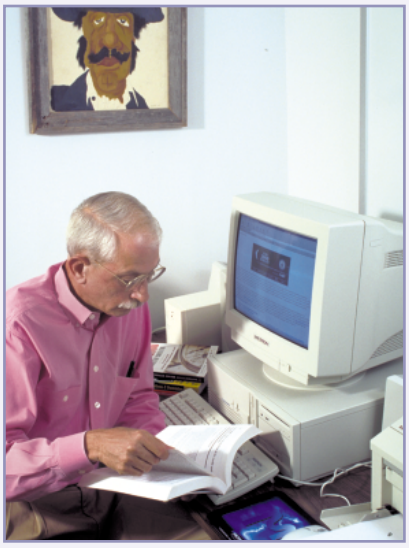
Requirements Collection for Forward-Looking Standards

This project focuses on the collection, coordination, and dissemination of federal technical requirements for cutting-edge software technology or for specifically identified problems that hinder interoperability efforts between federal agencies. Working with other federal agency representatives, ITL ensures that these requirements are made known to the appropriate voluntary standards community organizations. In FY 1999, the new Standards Working Group under the federal Chief Information Officers (CIO) Interoperability Committee held its initial meeting in December 1998 and a second meeting in April 1999. Working with two other federal agencies, ITL staff completed development of a draft Charter for the group, which was approved by the Working Group and the CIO Interoperability Committee. Members of the ITL staff continue to be directly responsible for the development of many different technical components in numerous information processing technology standards.

Role Based Access Control (RBAC)

This ITL project, shared with the Computer Security Division, is to design

and implement a security mechanism that reduces the effort for administration of complex security and access control problems in commercial systems. ITL developed the technical specifications for RBAC, including the formal description as well as a prototype implementation. We also developed an abstract and physical test suite to measure conformance to the RBAC model. In FY 1999, we co-sponsored the third ACM RBAC Workshop, which focused on the evaluation of the effectiveness of RBAC models and the development of new modeling concepts and techniques. These workshops bring together researchers, developers, and practitioners to discuss the application of RBAC to both traditional and emerging systems and the development of new modeling paradigms for future applications. Prominent companies represented include Oracle, Sybase, Tivoli, Intel, ICL, IBM, Data General, and Schumann AG. The Web site is http://hissa.nist.gov/rbac.



G. Fisher coordinates NIST standards and testing activities concerning the year 2000 computer problem. A major emphasis is creating awareness of the issues and possible solutions for overcoming the problems associated with converting systems and testing them for compliance with year 2000 date processing requirements.

VRML Conformance Testing

The Virtual Reality Modeling Language (VRML) is the file format standard for 3D-multimedia and shared virtual worlds on the Internet. ITL is building freely available diagnostic tools and conformance tests that will aid industry in building robust commercial solutions. We developed the VRML Test Suite (VTS) system and Viper, a VRML reference parser and scene graph generator. In FY 1999, we expanded the VTS by including interface tests. We also extended Viper functionality (Viper++) to include test case generation and test case evaluation capabilities. The Web site is http://www.nist.gov/vrml.html.

XML/DOM Conformance Testing

The Extensible Markup Language (XML) provides a standards-based approach to universal methods for defining and exchanging data. Using XML, one can create customized markup languages for exchanging information within their own domain. In addition, the Document Object Model (DOM) defines ECMAScript and Java bindings for interacting with XML and HTML data, permitting dynamic creation and manipulation of Web pages defined using these metalanguages. ITL co-chairs the OASIS XML Conformance Subcommittee. In FY 1999, we attended OASIS meetings and received industry support of our conformance testing efforts. We also defined an XML testing architecture, initiated tests and associated test environments, and initiated DOM testing. Web sites are http://www.oasis-open.org/committees/xmltest/testsuite.htm and http://bogey5.ncsl.nist.gov/dom/xmltest/.

Year 2000 (Y2K) Software Problem Information Dissemination

ITL provides a source of unbiased information concerning techniques that can be used to resolve Y2K software problems. We developed, and make available free of charge, software that can be used by organizations to evaluate their legacy software to attempt to determine the amount of potential exposure to Y2K failure that exists. Additionally, the Department of Commerce (DoC) emphasis on outreach to the information technology industry guided ITL to provide awareness presentations locally, nationally, and internationally in fulfillment of the DoC mission. In FY 1999, we participated in planning for the Y2K International Council. We assisted in the development of the DoC CD-ROM for Y2K outreach program. We developed an international status report on Y2K for online presentations. We also participated in the balloting process of IEEE 2000.2 recommended practice on Year 2000 Test Methods. We released Version 0.2 of FINDDATE scanner on our Web site. We participated in a panel on embedded systems and Y2K at a George Washington University conference on embedded systems and published a paper on embedded systems and Y2K. The Web site is http://www.nist.gov/y2k.

Statistical Engineering Division Projects

Bayesian Metrology

During the past decade with increased computing power and new research developments, Bayesian statistical methods have proven to be valuable tools in diverse areas of statistical applications. Bayesian methods provide a unified framework for optimally combining information from multiple sources, resulting in simpler and improved statistical analyses. After some preliminary research, NIST initiated a five-year competence initiative on Bayesian metrology in FY 1999. The goals of the project are to research, develop, and apply Bayesian methods to the metrological problems of NIST and to promulgate results to other metrology laboratories and to NIST customers. Four specific areas are targeted: traceability, interlaboratory comparisons, calibration, and part inspection. This year we completed a publication on a Bayesian model for interlaboratory comparisons, explored the relationship between the ISO uncertainty procedure and Bayesian statistics, and presented a review of Bayesian statistics to the NIST staff. NIST's Physics Laboratory and Manufacturing Engineering Laboratory collaborate with ITL on this project.

Statistical Reference Datasets (StRD) team - W. Guthrie, N. Zhang, P. Fagan, B. Rust, M. Vangel, J. Filliben, J. Rogers, C. Croarkin, E. Lagergren, L. Gill, and H. Liu.

Certification of Standard Reference Materials

The objective of this ITL project is to assure that certifications and uncertainty statements associated with NIST Standard Reference Materials (SRMs) are on a solid scientific foundation. SRMs are artifacts or chemical mixtures that are manufactured according to strict specifications and are certified by NIST for one or more physical or chemical properties of interest. NIST uses SRMs as a primary vehicle for disseminating measurement technology to industry. Division staff collaborate with NIST

scientists on validation of the measurement method, design of a prototype, stability testing, characterization of measurement error, and certification and uncertainty analysis. Statisticians advise on the design and analysis of experiments at all phases of this process. ITL typically handles the design and analysis of experiments for approximately 50 SRMs annually. Many of these SRMs are certified for multiple elements from two or three measurement methods whose differences must be reconciled and results combined to produce the certified values. SRMs are sold to industry for calibrating scientific instruments over an incredibly large variety of chemical, material, dimensional, and optical applications. NIST SRMs offer the highest level of accuracy for this technology transfer, and the success of the program depends entirely on the quality of the SRM certifications and their uncertainties.

NIST/SEMATECH Engineering Statistics Internet Handbook

NIST and SEMATECH, under a cooperative research and development agreement (CRADA), are collaborating on the development of an online Handbook of Engineering Statistics for distribution on the Web. Supported by SEMATECH and the NIST SIMA (Systems Integration for Manufacturing Applications) program, the project's goal is to produce an online resource that will be readily available and useful to engineers and scientists in industry, enabling them to incorporate statistical methods into their work more efficiently. Three other ITL divisions contribute expertise to the Statistical Engineering Division on this project. During FY 1999, we focused our efforts on creating chapter pages, assembling case studies with interactive computational capabilities, and integrating software with the handbook on multiple computer operating systems. Early in the year, we released the handbook for beta testing at NIST and SEMATECH. As reviews for each chapter were completed, ITL released the handbook to the public at the Web site http://www.itl.nist.gov/div898/projects/handbook.html.

Random number generation test development meeting with M. Smid, M. Levenson, A. Rukhin, J. Soto, E. Barker, and S. Leigh.

N. Zhang and M. Postek (MEL) discuss the quality of scanning electron microscope images.

Rockwell Hardness Standards

In today's metal products and materials industries, hardness testing is the most widely used mechanical test for quality control and acceptance testing. Rockwell C scale hardness indicates product properties critical to quality. The primary goals of this project are to provide U.S. industry with a means to make hardness measurements and calibrations with traceability to national standards and to facilitate acceptability of American hardness measurements worldwide. From a statistical perspective, NIST's objective is to enable people who do hardness measurement to judge the uncertainty in their measurements. This involves making available SRMs for the Rockwell C Scale, providing tutorials on experiments for judging the errors in hardness measuring systems, and extending this effort to other Rockwell scales. NIST SRMs for the Rockwell C scale went on sale in June 1998. In FY1999, NIST scientists presented tutorials on Rockwell hardness at the Measurement Science Conference and the National Conference of Standards Laboratories. A publication intended for the NIST Journal of Research on assessing hardness measurement uncertainty is in process. We also initiated work on SRMs for the Rockwell B Scale.

Industry Interactions

In partnership with industry, academia, and government, ITL pursues research areas of mutual interest. Through Cooperative Research and Development Agreements (CRADAs), we worked with 42 organizations in FY 1999. ITL also participates in many consortia and industry interest groups, including the following:

Advanced Television Systems Committee (ATSC)

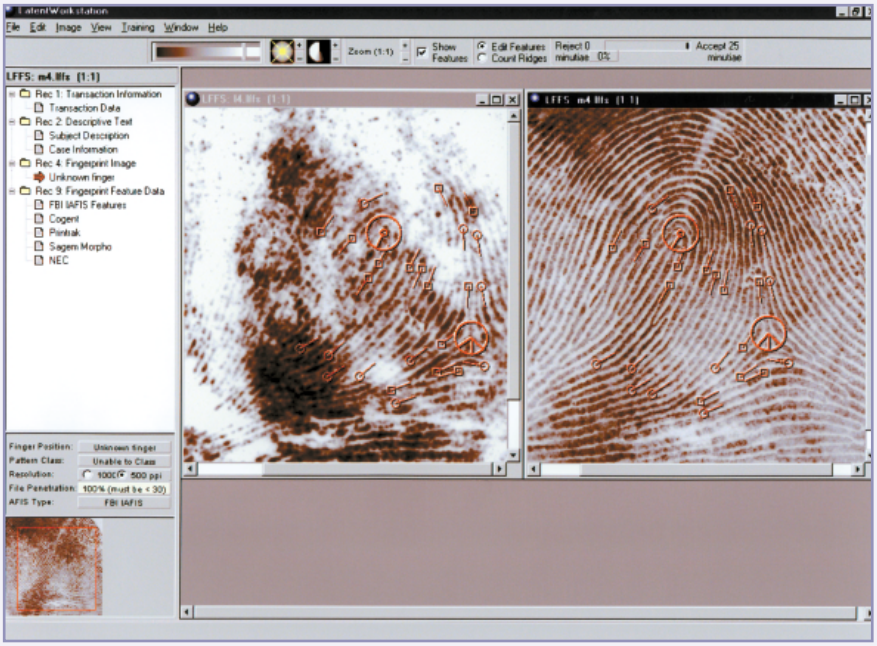
The ATSC was formed to establish voluntary technical standards for advanced television systems, including digital high definition television (HDTV). ITL staff members Alan Mink, Robert Snelick, Wayne Salamon, Alan Goldfine, Mark Skall, and Lynne Rosenthal participate in T3/S17, Digital TV Applications 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 test 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).



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.

Association for Computing Machinery (ACM)

Founded in 1947, ACM is the world's first educational and scientific computing society. ACM provides a vital forum for the exchange of information, ideas, and discoveries. Ronald Boisvert serves on the ACM Publications Board and as Editor-in-Chief of the ACM Transactions on Mathematical Software. John Barkley participates in the Role Based Access Control working group.

Association for Information and Image Management (AIIM) International

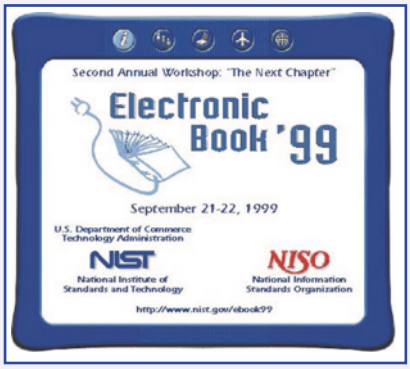
ITL participates in AIIM, the world's leading global association for information management professionals and providers of digital document technologies. Fernando Podio represents ITL on AIIM's Standards Board and Committee C21, Advanced Data Storage Subsystems.

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, and 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.

Center for National Software Studies (CNSS)

The CNSS is an organization of software professionals who recognize the need for national focus and informed leadership on software issues. ITL works with the CNSS to identify issues that affect the software capability of the nation. CNSS initiatives include national competitiveness, trustworthiness of software systems, and competency of the software workforce. Dolores Wallace represents ITL.

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; Tom Rhodes is the ITL contact.

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). William Mehuron and R.J. (Jerry) Linn represent NIST on the executive committee; other ITL representatives participate in working groups related to their research and development activities.

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 focuses 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 of electronic book reading systems. ITL also participates as a member of the Japanese Electronic Book Consortium effort. Dean Collins and Victor McCrary represent ITL.

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 the Java Scripting Language Study Group.

Foundation for Intelligent Physical Agents (FIPA)

FIPA is an international organization with the purpose of developing generic agent standards based on the participation of all players in the field. Tom Karygiannis and Wayne Jansen represent ITL.

IMS/EDUCAUSE

EDUCAUSE 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. Martha Gray and John Barkley participate in the project, Tom Rhodes serves on the Technical Board, and William Mehuron and Mark Skall serve on the IMS Advisory Board.

Information Technology Industry (ITI) Council

ITI is an industry association that represents the leading U.S. providers of information technology products and services. It promotes the global competitiveness of its 30 member companies. ITI serves as the secretariat for the American National Standards Institute (ANSI) Accredited National Committee for Information Technology Standards (NCITS) and as U.S. Technical Advisory Group (TAG) administrator for ISO/IEC Joint Technical Committee 1 on Information Technology. The ITL liaison is Michael Hogan.

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. Daniel R. Benigni is the ITL liaison to the IEEE Standards Association Board of Directors.

International Organization for Standardization (ISO)

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

International Telecommunication Union (ITU)

The ITU is an international organization within which governments and the private sector coordinate global telecom networks and services. Nader Moayeri represents ITL in the Bluetooth Special Interest Group.

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 actively participates in the Audio/Video Transport Area, Internet Area (IPv6, IP/ATM), the Management Area (SNMP, MIBs), the Multiparty Multimedia Session Control Area, the PKI Using X.509 Working Group, the Routing Area, the Security Protocols Area, the S/MIME Working Group, and the

Transport Area (RSVP, RTP). Doug Montgomery is the 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 and Craig Hunt represent ITL.

Java Grande Forum

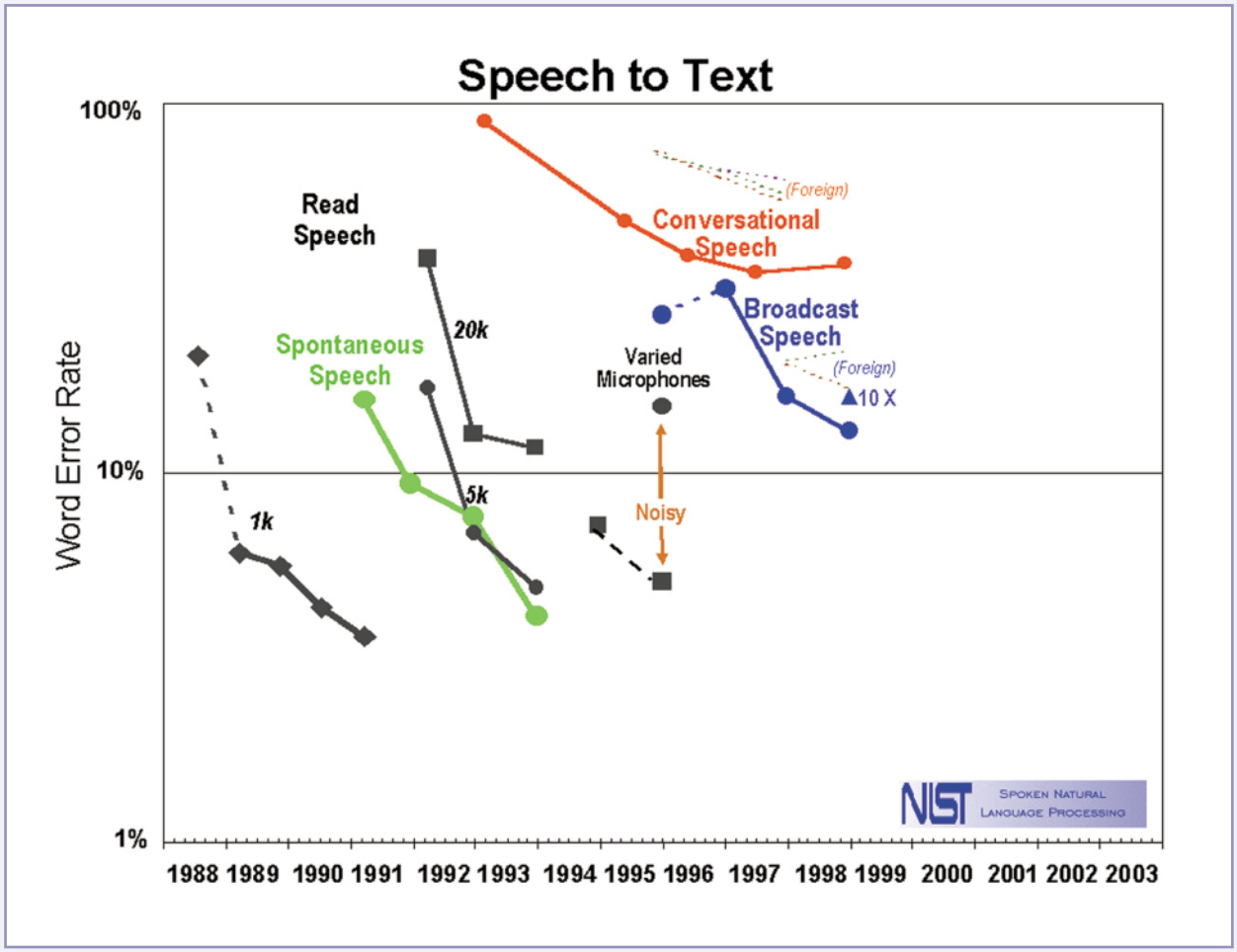
The Java Grande Forum (JGF) is an open forum of industrial, government and academic researchers, and software developers interested in improving the Java language and environment for use in high performance computing. Roldan Pozo and Ronald Boisvert co-chair the Numerics Working Group.

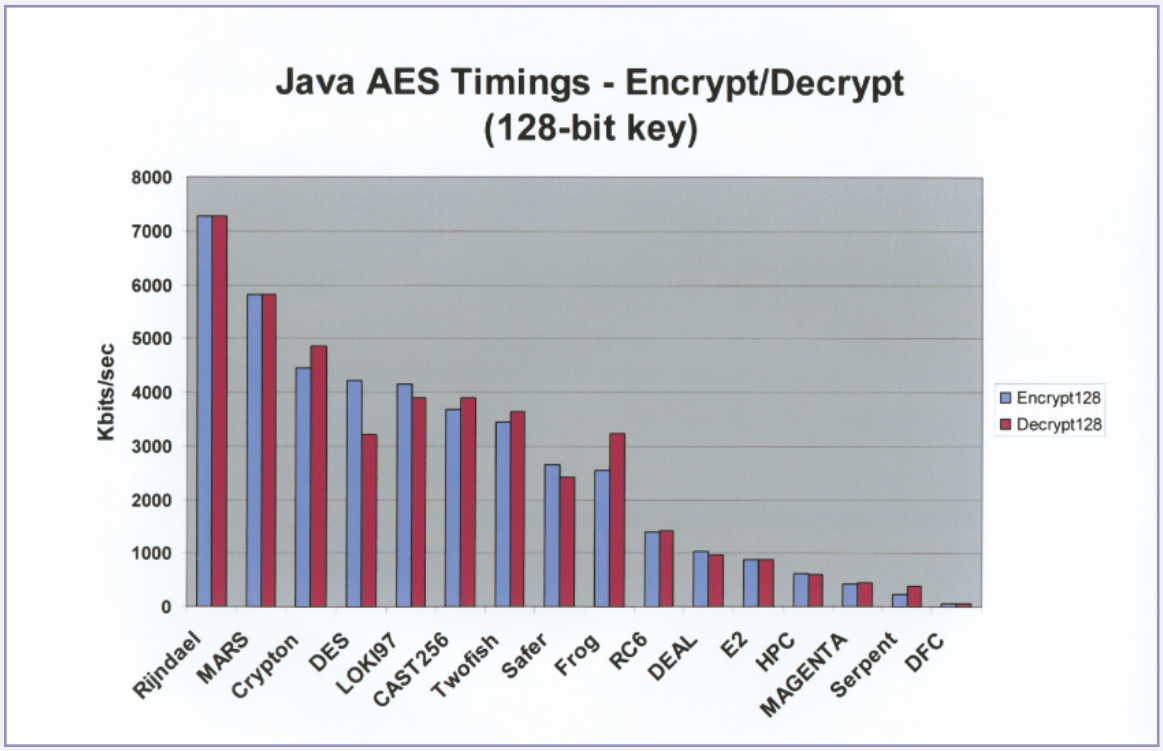
JTC1 TAG

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; Bruce Rosen participates in ISO/IEC JTC1 on Information Technology.

Micromagnetic Modeling Activity Group (muMAG)

The Micromagnetic Modeling Activity Group is an organization of industrial, government, and academic





researchers investigating fundamental issues in micromagnetic modeling through two activities: 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.

North American Integrated Services Digital Network (ISDN) Users' Forum (NIUF)

The NIUF is an industry/government consortium designed to create a strong user voice in the implementation of ISDN applications. Through the NIUF, users and manufacturers concur on ISDN applications and the resolution of issues, enhancing the strength of the U.S. telecommunications industry in the world marketplace. ITL's Leslie Collica chaired the NIUF until the workshop activity concluded in July 1999.

North America OpenMath Initiative (NAOMI)

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

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 and Bruce Rosen represent ITL. Michael Hogan serves on the NCITS Policy and Procedures Committee. ITL staff participate in many technical working groups of this organization.

Participation in management activities includes Thomas Ndousse-Fetter and David Cypher in T1, Telecommunications, and Donna Dodson and Tim Polk in X9, Financial Services.

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 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. ITL contributes to three working groups within OMG. A member of the OMG Object Management Group, John Barkley is ITL's principal representative.

OPEN GROUP

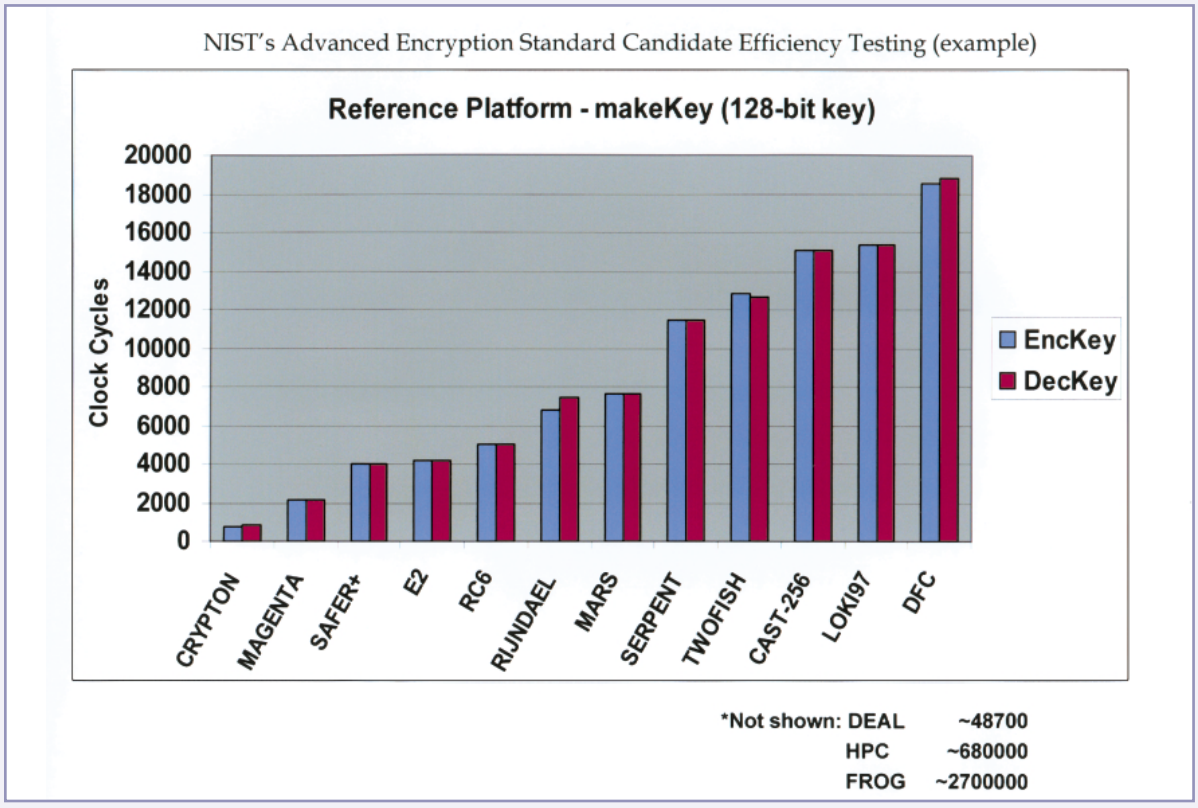
The OPEN GROUP was established to aid in the development and implementation of a secure and reliable IT infrastructure. Shu-Jen Chang participates in Security Services.

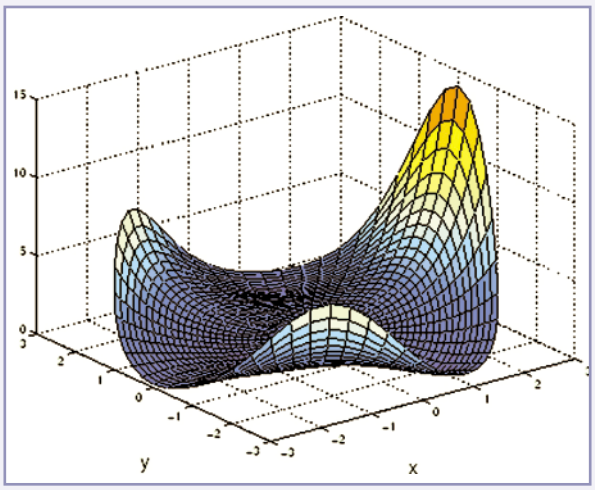
Optical Internetworking Forum (OIF)

Thomas Ndousse-Fetter and David Su participate in the Architecture, Internetworking, and Management Group.

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.





This image shows the modulus of the complex Airy function Bi (z) in the vicinity of the origin. The Airy functions are one of the special functions described by the Web-based Digital Library of Mathematical Functions being developed by ITL.

Real-Time Java Expert Group

The Real-Time Java Expert Group operates under Sun Microsystem's 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.

Software Engineering Body of Knowledge Industrial Advisory Board

ITL serves on the Industrial Advisory Board for the ACM and IEEE Computer Society's project to develop a Software Engineering Body of Knowledge (SWEBOK). The purpose of the SWEBOK is to identify the body of knowledge of software engineering and to provide suitable access to that knowledge. Dolores Wallace and Larry Reeker represent ITL.

Software Engineering Institute (SEI)

The SEI is a research and development center with a broad charter to address the transition of software engineering technology. ITL established a memorandum of understanding with SEI to work collaboratively on software engineering issues of mutual interest. Dolores Wallace is the ITL principal.

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, develops laboratory implementations of proposed interface architectures, and develops metrics. John Roberts represents ITL in this organization.

Web3D Consortium

The Web3D Consortium provides an open forum for the creation of open standards for Web 3D specifications and accelerates the worldwide demand for products based on these standards through the sponsorship of market and user education programs. Through participation in the Web3D Consortium, ITL works with industry to develop conformance tests and test tools for VRML. 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, Mary Brady, and Tim Boland represent ITL.

International Activities

Common Criteria (CC)

As part of the National Information Assurance Partnership (NIAP), NIST has been engaged in a cooperative project with the National Security Agency and the governments of Canada, France, Germany, Netherlands, and the United Kingdom to develop the CC for Information Technology Security. The CC provides the structure and components to describe standardized security requirements for all types of computer-related products. These requirements can be used as the basis for performing security testing and evaluation of such products. The Mutual Recognition Arrangement signed on October 5, 1998, allows U.S. manufacturers to sell their evaluated, security-enhanced IT products to Canada, France, Germany, and the United Kingdom without duplicate, costly evaluations in each of these importing nations.

Encryption (128-bit key)

Best results - clock cycles; 200MHz Pentium Pro

	NIST [1]		[Gladman] (Table 1)		[Schneier] (Table 2)	
	Clock Cycles	Rank	Clock Cycles	Rank	Clock Cycles	Rank
CAST-256	2169	10	633	6	660	6
CRYPTON	579	1	474	5	476	5
DEAL	3197	12	2339	13	2600	13t
DFC	3491	13	1642	10	1700	11
E2	1523[2]	6	687	7	720	7
FROG	1611	7	2417	14	2600	13t
HPC	9401	15	1429	9	1600	10
LOKI97	3077	11	2134	12	2150	12
MAGENTA	9253	14	6539	15	6600	15
MARS	807	3	369	2	390	2
RC6	636	2	270	1	260	1
RIJNDAEL	809[2]	4	374	3	440	4
SAFER+	2095	9	1722	11	1400	9
SERPENT	1629	8	952	8	1030	8
TWOFISH	973[2]	5	376	4	400	3

[1] blockEncrypt (NULL Cipher) = 41 clock cycles
[2] BC results (fewer cycles than MSVC)

The CC Project has also worked very closely and interactively for the last five years with the International Organization for Standardization (ISO) to help the CC become a three-part International Standard. That work came to fruition in June 1999 when the ISO National Bodies balloted to accept the CC as International Standard 15408, an event which has been awaited by numerous nations and computer product manufacturers throughout the world. The CC has already been translated into French, German, Russian, Japanese, Korean, and other translations are in progress. ITL's Gene Troy, who was one of the organizers of the CC Project and an author of the CC, is ISO Project Editor of Part 1 of the new standard.

Database of Software Faults and Failures

ITL is developing a repository for Reference Data on Software Faults and Failures. The project includes development of tools for the collection and analysis of data by software developers, to help the software industry identify the types of faults that occur in different kinds of software. In FY 1999, a guest researcher from the Egyptian National Institute of Standards 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. Dolores Wallace is the ITL contact.

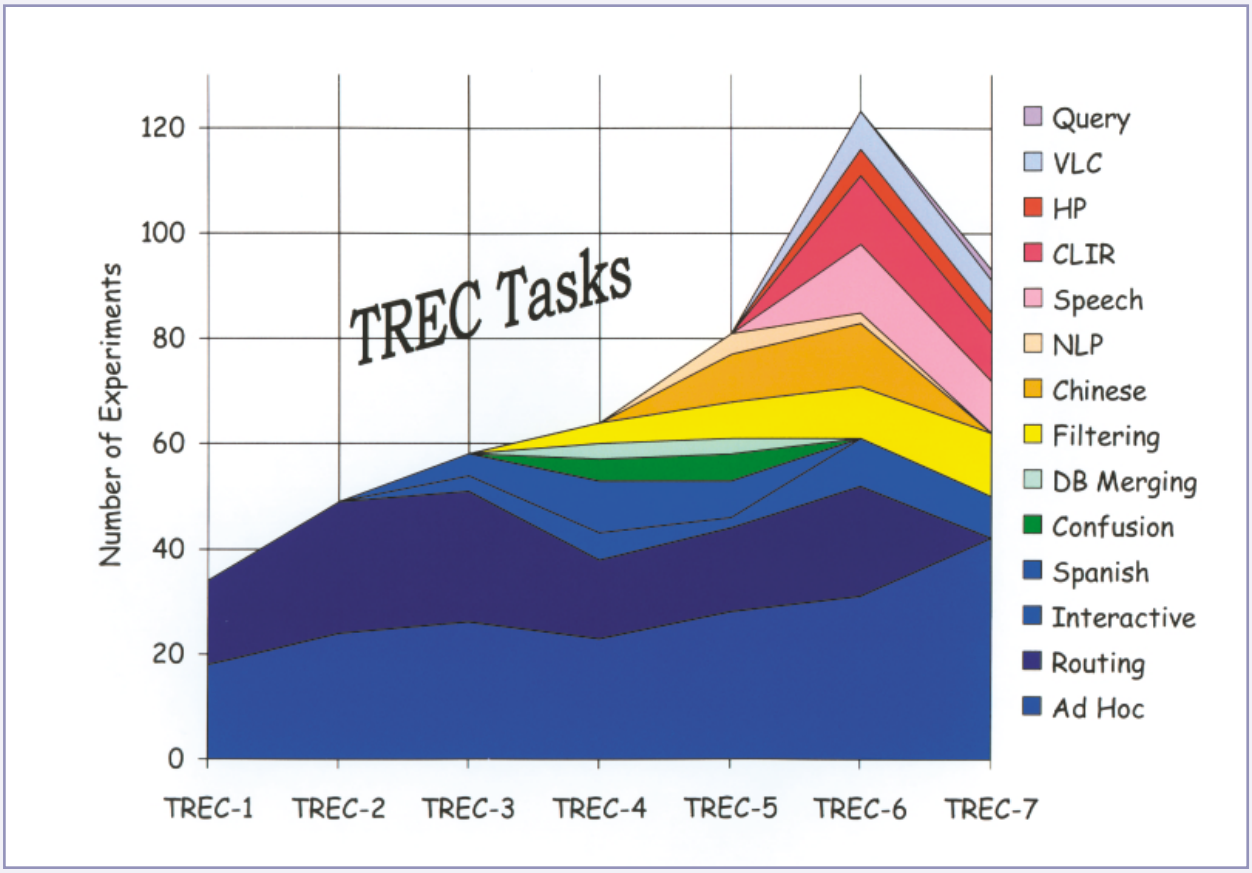
G8 Information Society Pilot Projects

The G8 Information Society started as a coalition of the major industrialized nations and has expanded to include a large number of other countries and organizations. Its mission is to build on and sustain the process of globalization and to ensure that its benefits are spread more widely to improve the quality of life of people everywhere. ITL provided leadership in planning, developing, and implementing the U.S. contributions to two of the eleven Pilot Projects: the Global Inventory Project (GIP) and the Global Marketplace for Small and Medium Enterprises (SMEs). Judi Moline serves as the U.S. representative to the two steering committees and as co-chair of the SME project. The pilot phase of these projects will end late 1999. In summary:

- The GIP cooperation resulted in a Web site that provides a single, multilingual window to a large number of projects on distributed servers related to the Information Society. Its original and transferable solutions add value to similar initiatives carried out by other countries and illustrates innovative information technologies and best practices. Again there is interest in continued work.

- The SME pilot contributed to electronic commerce policy and actions in most of the participating countries. It also sparked an international dialogue. There is no doubt about interest in continued work on the global marketplace for SMEs. There is no other private/public sector forum where "policy meets practice," that is, where the practical implementation of electronic commerce tools and policy affecting SMEs is its focus.

One of the important lessons learned by the G8 Pilot Project experience has been that there is great willingness to work



together; however, for international cooperation to be effective and result in concrete projects, at least a minimal budget should be available. Actions require the presence of some kick-start public funding, which can then attract private funding. In the case of the SME and GIP pilot projects, the participating entities cooperated by providing technical leadership and Web sites with appropriate content. Additionally, the European Commission provided the Secretariats and seed money to kick-start special events.

International Federation for Information Processing (IFIP)

ITL participates in the IFIP Working Group on Numerical Software (WG 2.5), which is part of the IFIP Technical Committee on Programming Languages (TC 2). The aim of Working Group 2.5 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 May 1999, for example, WG 2.5 formally endorsed the work of the Java Grande Forum. Ronald Boisvert represents ITL.

Japan's Electrotechnical Laboratory

The Mathematical and Computational Sciences Division is collaborating with Japan's Electrotechnical Laboratory (ETL) on the design of high performance mathematical software for numerical linear algebra. As part of this work, ETL developed and maintains a mirror Web site for the Matrix Market in Asia, including a visual database of large sparse matrices from industrial applications, while NIST is incorporating interactive matrix generation software from ETL into the Matrix Market. Ronald Boisvert and Roldan Pozo represent ITL.

Text Retrieval

ITL's Text REtrieval Conference (TREC) series, which focuses on the creation, administration, and analysis of large, complex data collections, has inspired groups in other countries to try similar evaluation efforts. The NACSIS (National Center for Science Information Systems), a Japanese government organization, held its first workshop in August 1999, and a group in France and one in Korea are also planning workshops. Each group cited TREC as their model and asked NIST for guidance and advice. Donna Harman is the ITL contact.

Year 2000 (Y2K) Issues

In November 1998, ITL proposed recommendations to government and industry representatives of Costa Rica on Y2K issues. Gary Fisher, a member of the Software Diagnostics and Conformance Testing Division, keynoted a Y2K conference in San Jose, Costa Rica, which was sponsored by the Colegio de Profesionales en Informatica y Computacion. Attended by 300 information technology professionals from Costa Rican industry and government, the conference featured talks by the Costa Rican Ombudsman for the Citizenry and the Deputy Minister of Science and Technology who chairs the country's task force for Y2K conversion. Fisher also spoke on Y2K issues and international readiness to meet the challenge at the International Conference on Gallium Arsenide Manufacturing Technology (GaAS MANTECH) in Vancouver, B.C., in April 1999.

NIST Y2K WEB SITE

Staff Recognition

Department of Commerce (DoC) 1999 Medal Awards

Paul D. Domich, ITL's Assistant Director for Boulder, received the DoC Bronze Medal for leadership in enhancing NIST's information technology services.

Donna K. Harman, manager of the Natural Language Processing and Information Retrieval Group, Information Access and User Interfaces Division, was recognized with the DoC Bronze Medal for initiating, developing, and leading the Text Retrieval Conferences, the premier evaluation program in the text document retrieval community.

Mary C. Brady, Software Diagnostics and Conformance Testing Division, was awarded the DoC Bronze Medal for leadership in developing the industry-endorsed and internationally recognized Virtual Reality Modeling Language (VRML) conformance testing program.

Jeanne Springmann, Distributed Computing and Information Services Division, was part of a group that received a DoC Bronze Medal for the development and implementation of a database system for the comparison of international measurement standards and national systems of traceability.

External Staff Recognition

Anthony J. Kearsley, a research mathematician in ITL's Mathematical and Computational Sciences Division, received the prestigious 1998 Presidential

Paul D. Domich

Donna K. Harman

Mary C. Brady

Jeanne Springmann

Early Career Award for Scientists and Engineers. The award recognizes his work in the development and use of large-scale optimization techniques for the solution of partial differential equations arising in science and engineering. Spanning the areas of problem formulation, algorithm design and analysis, as well as computer software development, the wide impact of Kearsley's work has been quite remarkable. His contributions have allowed advances in such diverse areas as oil recovery, antenna design, wireless communications, climate modeling, and high temperature superconductors. Kearsley is the second ITL scientist to be recognized by the Presidential Early Career Award for Scientists and Engineers since its inception by President Clinton three years ago.

Anthony J. Kearsley

Mark G. Vangel, a mathematical statistician in the Statistical Engineering Division, was designated a Fellow of the American Statistical Association (ASA) at the Association's annual meeting in August 1999. Each year members of the ASA make nominations from among their peers for this honorary title, which recognizes outstanding contributions in some aspect of statistical work.

Mark G. Vangel

The Association for Information and Image Management (AIIM) International awarded ITL's **Fernando L. Podio** the 1999 National Standards Leadership Award in recognition of his dedication, guidance, and leadership in the AIIM International Standards Program. AIIM International is the leading global association bringing together information management professionals and providers of digital document technologies.

The National Security Agency (NSA) selected Miles E. Smid, Acting Chief, Computer Security Division, as a finalist for the Frank B. Rowlett Trophy (NSA's INFOSEC National Awards) for Individual Achievement. *(Winners were not announced in time for inclusion in this report.)*

Fernando L. Podio

Service to NIST

ITL provided a wide spectrum of supporting and consulting services to NIST staff in FY 1999, including:

COMPUTING SUPPORT TO THE NIST STAFF

Our NIST customers received a wide range of scientific and administrative computing support from ITL, including the following:

- an easy-to-use, robust, secure, 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 application software;
- site-wide hardware maintenance for standardized desktop systems and workstations and site-wide software licensing;
- maintenance and repositories for standardized platforms and applications;
- large-scale testbeds, advanced prototypes, and reliable systems as part of the continuous improvement in scope and quality of service;
- a powerful scientific computing capability, which encompasses shared-memory parallel systems including three powerful SGI 2000 Origins, each with 32 processors and 32 Gigabytes of memory, and one 8 CPU Origin 2000. Distributed-memory parallel computing is handled by a newly upgraded 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. Consulting and training are available to complement a substantial collection of popular software packages; and
- networking and telecommunications support.

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 NIST's mission. This work ranges from short-term consultations to long-term collaborations. Some examples of cooperative projects follow. ITL researchers are

P. Ketcham, B. am Ende, T. Griffin, R. Bohn, B. George, H. Hung, and J. Hagedorn discuss their support to NIST scientists on a wide range of computer and software topics.

- applying triangulated irregular networks to the processing of lidar scanning data from construction sites. This work helps Building and Fire Research Laboratory (BFRL) engineers in developing techniques for the automated assessment of construction progress.

- collaborating with the Manufacturing Engineering Laboratory (MEL) and the Physics Laboratory (PL) in the study of high-speed machining processes. ITL is studying nonlinear dynamics of the simulation of aluminum cutting, with the goal of predicting the onset of instabilities.

- working with Materials Science and Engineering Laboratory (MSEL) scientists to establish new acoustic microscopy techniques that will allow the determination of stresses in ceramic materials. ITL is extending the theoretical model of this technique to anisotropic solids and curved surfaces.

- developing, with colleagues in the Chemical Science and Technology Laboratory (CSTL), probabilistic methods for the analysis of genome data. Such work is of interest in the development of metrics for classification in genomic databases.

- working with colleagues in the Electronics and Electrical Engineering Laboratory (EEEL) on the modeling of optoelectronic components of interest in the telecommunications industry. The development of rigorous models and reliable solution algorithms for the simulation of diffraction gratings used in optical waveguides is in process.

- cooperating with BFRL on fluid flow in complex geometries. Additional collaborative work with BFRL concerns modeling high performance concrete. In both cases, the parallel code enables runs of very large size.

- working with PL on optical absorption due to excitons. The parallel code enables the use of a new theory to predict optical properties in semiconductors and insulators.

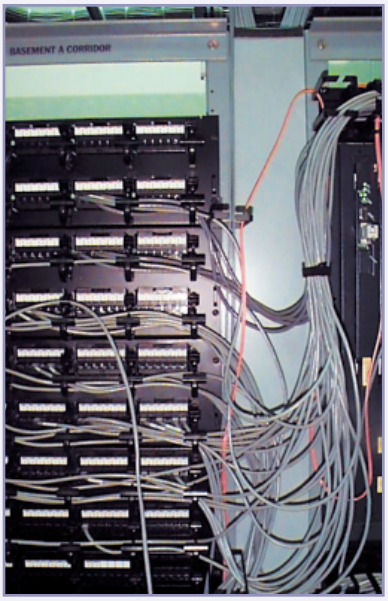
- developing, with MSEL, parallel algorithms for dendritic growth in metallic alloys. This resulted in a new load-balancing algorithm for our DParLib parallel library.

In the continuing upgrade of the NIST scientific computing facility, ITL added two new 32 CPU, 32 gigabyte memory, SGI Origin 2000 systems. R. Schaffer examines the system which provides a robust memory configuration in a symmetric-multiprocessing (SMP) environment.

- working with PL in visualizing vortices in Bose-Einstein Condensate under rotation. This three-dimensional visualization has been converted to stereo, which enables a clear view of the vortices.

- developing statistical methods for characterization of high-speed oscilloscopes in collaboration with researchers in EEEL, Boulder. These methods are needed for a project characterizing how photodiodes distort optical communication signals.

- collaborating with MSEL to develop a modified maximum likelihood procedure for estimating the failure-time distribution of copper piping joints. Using this method, researchers can study the strength of joints made with various lead-free solders.
- making an important contribution, with MEL, to automated measurement of the sharpness of Scanning Electron Microscope images. Several companies in the semiconductor industry expressed interest in using this methodology in their instrumentation, and Spectel R&D Co. implemented it in their workstations.
- collaborating with researchers in MEL on the development of statistical methods to analyze and calibrate Coordinate Measuring Machines.



SELECTED CONFERENCES, WORKSHOPS, AND TRAINING COURSES

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

12th Federal Information Systems Security Educators' Association (FISSEA) Conference

21st National Information Systems Security Conference

Advancing Measurements and Testing for Information Technology

Atomistic Modeling at NIST

Biometrics Consortium Fall '99 Conference

BLAS Technical Forum

Electronic Book '98 and '99

Fifth Conference on Human Factors and the Web: The Future of Web Applications

Indexing Techniques for Image Databases

Interoperable Message Passing Interface (IMPI) Standard Workshop

ITL Seminar Series

Mathematical and Computational Sciences Division (MCSD) Colloquia

NIST Director's Workshop on Being the Best in the World: Developing Measurements and Standards for Secure Cryptographic Systems

Non-Numerical Methods for Scientists and Engineers

North American ISDN Users' Forum (NIUF)

Potential for Fingerprint Template Standards for Authentication Applications

Scientific Computing at NIST: An Orientation to Resources

Second Advanced Encryption Standard (AES) Candidates Conference

Second International Conference on Audio and Video-Based Person Authentication

Seventh Text REtrieval Conference (TREC)

Statistical Engineering Division Case Studies Series

Statistics for Scientists and Engineers - Analysis of Variance, Uncertainty Analysis

White Hat Guide to Network Security and Vulnerability Testing

Workshops on Real-Time Java Implementation Issues

Workshop on Role Based Access Control

ITL publishes a variety of publications, newsletters, bulletins, and documents online. The Web site is http://www.nist.gov/itl/lab/csl-pubs.htm. A link to information about FY 1999 ITL research papers and other publications can be found at this Web site.

Patch panel connected to the NIST Local Area Network (LAN). Each Ethernet port on this panel corresponds to an Ethernet jack in a user's office. Activation of ports can be requested through a Web form.

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.*