

NIST Networking and IT Research

Dr. Susan F. Zevin Acting Director Information Technology Laboratory National Institute of Standards and Technology





Outline

- NIST Overview
- Importance of Standards
- Methodology
- Scale: Space and Time Considerations
- Theme: Trust and Confidence
- Selected Efforts
- Challenges
- Resources





"The ability to extend the frontiers of discovery is increasingly reliant on technology. Powerful computing and further development of IT are the enabling forces behind the revolution in research unraveling the structures of life on the micro-scale and structures of the universe on the macro-scale."

> Dr. John H. Marburger, Director of the Office of Science and Technology Policy, President's Science Advisor

"Strengthening National, Homeland, and Economic Security," Networking and Information Technology Research and Development, Supplement to the President's FY 2003 Budget, National Science and Technology Council, July 2002





The National Institute of Standards and Technology (NIST)





NIST Assets Include:

NIST Laboratories -- National measurement standards

- 3,000 employees
- 1,500 technical staff
- 1,600 guest researchers
- Unique measurement and research facilities
- Joint institutes with universities

Extramural programs

- Advanced Technology Program -- \$640 million current R&D partnerships with industry
- Manufacturing Extension Partnership -- 400 centers nationwide
- Baldrige National Quality Award

NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.





NIST's Measurement and Standards Laboratories





NIST Products and Services

- Measurement Research 2,200 publications/year
- Standard Reference Data 65 types available 5,000 units sold/ year
- Standard Reference Materials

 >1,300 products available
 30,000 units sold/year
- Calibrations and Tests >3,000 items calibrated/year
- Laboratory Accreditation 764 accreditations
- Standards Committees 400 NIST staff, 900 committees







Importance of Standards









Without Standards...







*TI*³ = Trustworthiness, Interoperability, Integration, and Intelligence

National Security Interoperability Integration Intelligence Trustworthiness

Health Care Interoperability Integration Intelligence Trustworthiness

Web Services Interoperability Integration Intelligence Trustworthiness

Finance Interoperability Integration Intelligence Trustworthiness

Manufacturing Interoperability Integration Intelligence Trustworthiness





Methodology

Standards Roadmap: Approach

- Collaboration with industry to define and demonstrate a framework and prototype

 Can be adopted and extended by others
- Work with the community
 - Identify stakeholders, roles, use cases
 - Identify relevant standards, organizations
 - Identify existing and similar efforts
- Define the metadata, taxonomies, and information model
- Develop framework infrastructure and web services
- Demonstrate and deploy

NIST Expectations and Drivers

Scale:

Space and Time Considerations

Spatial Resolution

Electronics

National Institute of Standards and Technology

Small: Single Molecule Manipulation and Measurement (SM³)

Developing and integrating new measurement methods to transport and probe structure, function, and dynamics of single biomolecules

DNA, RNA, and Proteins

Smaller: Quantum Information Science

Confluence of two revolutions of the 20th century: *computer science and quantum physics* Paradigm shift: information as a physical quantity

Implications for homeland security

Perfectly secure defense communications Ability to solve problems impossible to compute today Codebreaking Pattern matching

Implications for commerce and trade

Secure electronic commerce Maintenance of lead in computer technology marketplace

From Modeling to Visualization and Metrics

Modeling of aggregates for more realistic computations and visualization

Visualization of hydrating cement at submicrometer resolution

Modeling and visualization of (for accurate studies of service life

From Modeling to New Observing Systems

Modeling and visualization of the flow of suspensions

Modeling and visualization of flow through rebars to ensure that concrete can be placed properly

Study of flows in rheometers to enable better designs

Virtual Experimentation and Visualization: Higher Performance Materials

- Tools to optimize the performance characteristics
- Software for performing lifecycle cost analysis
- Web-based software system for virtual testing and optimization

National Institute of Standards and Technology

Four Themes for the Future:

Trust and Confidence Complex Systems e-Knowledge e-Science

it

In specification development

- Consequences of poor spec definition
 - In company specs \$ (assuming problem found downstream)
 - In standards development (whole industry decides to reiterate)
- Projects (research)
 - formal spec methods can be tied to automated test development (save \$) (Outcome: Ford is using, consortia created) (Project in tech transfer stage)

National Institute of Standards and Technology

- Success in using semi-formal language in standards process.

In system testing

- Consequences
 - Desired Functionality not achieved
 - Vulnerable systems
- Projects: (Conformance/certification efforts)
 - XML testing
 - Security certifications

In system implementation

- Consequences
 - System level:
 - Stolen info, untrusted info, info not available
 - Loss of/confusion of data in information exchange
 - Application level:
 - Lack of confidence in calculations/measurements
 - Decisions based on bad information
- Our Approach: (Standards collaboration)
 - Security standards
 - Preventing wireless collisions (through standards)

In Cyber Security

- Cryptographic Standards and Applications
 - Advanced Encryption Standard (AES)
 - CMVP (Cryptographic Module Validation Program)
 - Cryptographic Standards Toolkit
 - Key management
- NIAP (National Information Assurance Partnership)
 - to foster the availability of objective measures and test methods for evaluating the quality of Information Technology (IT) security products
 - development of commercial testing laboratories that can provide the types of testing and evaluation services which will meet the demands of both producers and users.
- Security for Emerging Technologies
 - Smart cards (authentication, interface to PDAs, etc.)
 - Guidelines (smart card, VOIP, anti-virus tools, etc.)

In Data Preservation

- Testing methods for data storage devices and media
- Integrated vision of data en/decapsulation, transfer, voice/video/text format integration, ensuring continuity of fidelity/quality
- Architecture for long life "cyber-storage" of personal data, through several system life cycles

National Institute of Standards and Technology

Understanding and Control of Complex Systems

The interconnected characteristics of a complex system need...

Heterogeneity Connectedness Large state space Continuous Change Unpredictable scalability Open-endedness Unpredictable human element

...Systems level understanding with certain component and system characteristics

> Real-time Self-adaptive Self-organizing Self-healing

Future Networks: Dynamic Flexibility, High Bandwidths, and Security

Challenge: Scalable technology for massive increases in heterogeneous network traffic including billions of wireless devices and sensors

Research Focus

 Developing and prototyping next-generation technologies to dramatically increase the speed, reliability, security, and versatility of large-scale and broadband networks

Integration of pervasive computing technologies for future systems

- Modeling and measurement of pervasive systems
- Integration software to facilitate pervasive systems
- Interference and coexistence techniques for wireless communication protocols
- Dynamic service discovery

National Institute of Standards and Technolog

Information Delivery Systems

- Networked Communication of Pervasive Computing Devices
- Metrics and Protocols for Ad Hoc Wireless Networks
- Agile Switching Infrastructures
- Internet Infrastructure Protection
 - DNS and IP Security

e-Knowledge: Finding, Analyzing, and Utilizing Data

ate

There must be some easy way to find that needle...

Advanced Technologies to Build Knowledge from Data

- Challenge of the Information Tsunami
 - Organizing and utilizing quality information from heterogeneous sources in real time to optimize decision making
- Research focus: Next-generation, interactive information technologies that not only store and organize information, but can help people find and see the significance of and interact with the information they need

Computer Forensics

 National Software Reference Library – standard reference data set of file signatures (hash) of COTS files used during examination of digital evidence to allow identification of pertinent files and elimination of others

 Computer Forensics Tool Testing – verification of computer forensic tools and their use in analyzing digital evidence used to ensure tool usage yields objective, repeatable, reproducible, results that meet the requirements of the user and are admissible in court

Supporting the health care industry

Standard Reference Information:

- cholesterol and other blood components
- properties of medical implants
- alcohol level (breath and blood)
- nutritional status (vitamins and minerals)
- toxic substances in urine
- drugs of abuse
- DNA profiling

ATL

- radioactivity-measuring instruments
- calibration of medical lab tests

Supporting the health care industry Dosimetry

Mammography calibrations

- 26 million mammograms/year
- 11,000 facilities

Calibration of radioactive sources for treatment of cancer and heart disease

- 180,000 prostate cancers/year
- 600,000 angioplasties/year

Biometrics

- USA PATRIOT Act of 2001 and Enhanced Border Security and Visa Reform Act: NIST to work with Departments of Justice and State to "develop and certify a technology standard" for biometric identification of persons entering the U.S. or applying for visas
 - Automated identification and matching of fingerprints, facial features, and other biometric information
 - Interoperability of biometric databases and systems
 - Biometric systems performance metrics

Human-Computer Interaction: Broadening IT Capabilities to Support Human Needs and Goals

Challenges:

- Make computing capabilities and devices easier for all people to use
- Develop technical innovations that broaden the range and types of services IT can provide

Research Areas

System Standards

- Usability
- Human Languages
- Accessibility
- Human factors

BALLOT, GENERAL ELECTION BEACH COUNTY, FLORIDA NOVEMBER 7, 2000		A		OFFICIAL BALLOT, GENERAL EI PALM BEACH COUNTY, FLO NOVEMBER 7, 2000
(REPUBLICAN) GEORGE W. BUSH - PRESIDENT DICK CHENEY - VICE PRESIDENT	3₩	0.0	4 4	(REFORM) PAT BUCHANAN PRESIDENT
(DEMOCRATIC) AL GORE - PRESIDENT JOE LIEBERMAN - VICE PRESIDENT	5->	0.0		EZOLA FOSTER INCLIPRESIDENT (SOCIALIST)
(LIBERTARIAN) HARRY BROWNE PRESIDENT ART OLIVIER -VICE PRESIDENT	7>	000		MARY CAL HOLLIS - VICE PRESIDENT (CONSTITUTION)
(GREEN) RALPH NADER - PAISIONT WINDNA LADUKE - VICE PRESIDENT	9	9 69 6		J. CURTIS FRAZIER - VICE PRESIDENT (WORKERS WORLD)
(SOCIALIST WORKERS) JAMES HARRIS - PRESIDENT MARGABET TROWE - WEE PRESIDENT	11>>			GLORIA LA RIVA VICE PRESIDENT
(NATURAL LAW) JOHN HAGELIN PRESIDENT NAT GOLDHABER WICE PRESIDENT	13>>	8		To vote for a write in candidate, follow the directions on the long stub of your ballot card.

National Institute of Standards and Technology

Computation at the Frontiers of Complexity

- Challenges:
 - High performance computer architecture
 - Revolutionary and innovative processing and storage concepts
 - System software
 - High-end algorithms and codes for scientific computation
 - Integrated and optimized software infrastructure for distributed computing environments

Build expertise in algorithms and software

- Libraries for data management in parallel applications
- Research in object-oriented software design, e.g. micromagnetic modeling, modeling of materials with complex microstructure

Community-developed software system standards

- Interoperable Message Processing
 - Standardizing message passing to heterogeneous clusters
- Sparse Basic Linear Algebraic Systems
 - Standardizing programmer interface to core linear algebra operations central to most large-scale models
- Java Numerics
 - Working to improve the Java language and environment for high performance scientific computing

Measurements and standards for future generation computer architectures

- Semiconductor metrology
- Metrology for optical communications
 - Characterize properties of optical sources & detectors for 40 Gbit/sec time division multiplexing systems
 - Protocols for high-speed optical networks
- Quantum computing and communications
 - Quantum memory, processors, architectures, error correction, algorithm development
 - Testbeds for quantum key distribution

Resources

(PT

 \mathcal{D}

http://www.nist.gov/ http://www.itl.nist.gov/

