



Research and Development for Secure and Trustworthy Information Systems

presented by
Cita M. Furlani

**Director, Information Technology Laboratory
National Institute of Standards and Technology**

**DHS-DOD-NIST
Software Assurance Forum
National Institute of Standards and Technology
Gaithersburg, MD
October 14, 2008**



NIST Mission

To promote U.S. innovation and industrial competitiveness by advancing

- measurement science,
- standards, and
- technology

in ways that enhance economic security and improve our quality of life

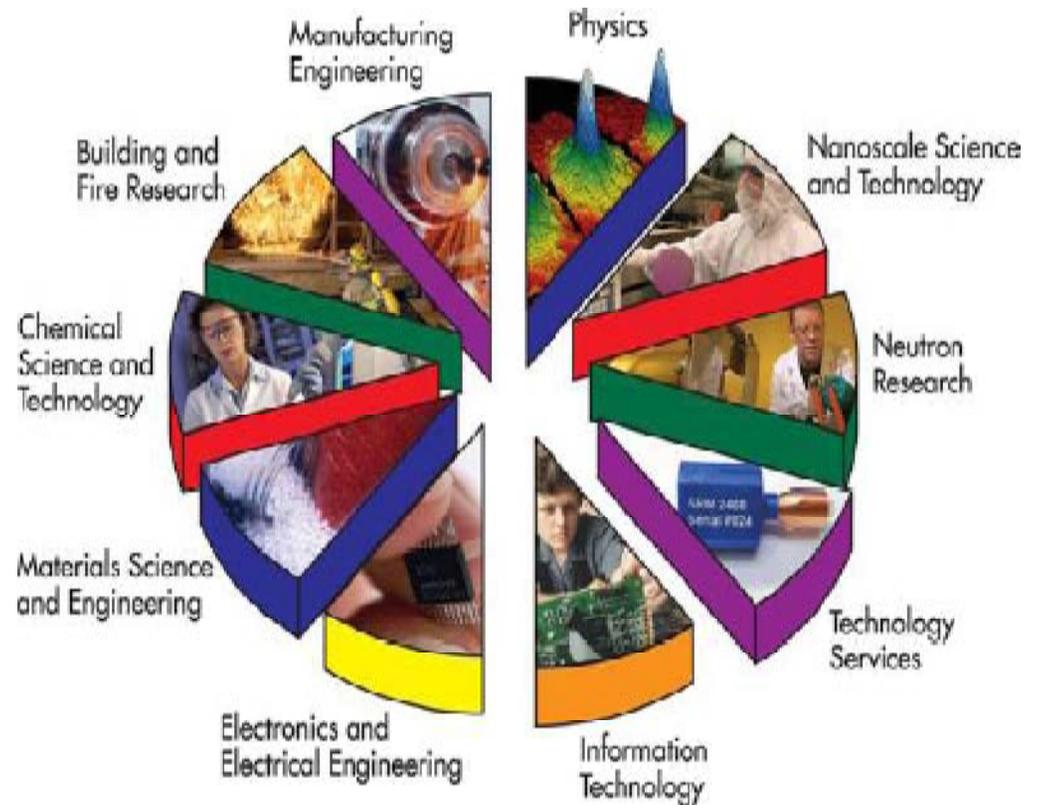


NIST's work enables

- Science
- Technology innovation
- Trade
- Public benefit

NIST works with

- Industry
- Academia
- Other agencies
- Government agencies
- Measurement laboratories
- Standards organizations





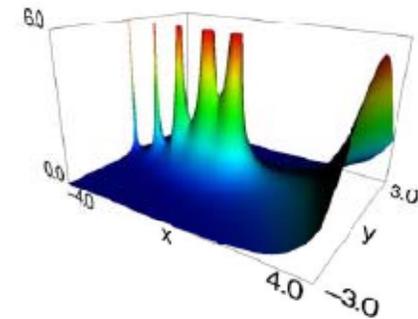
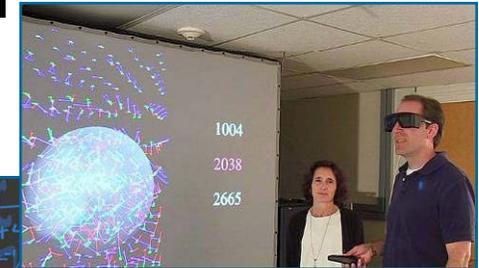
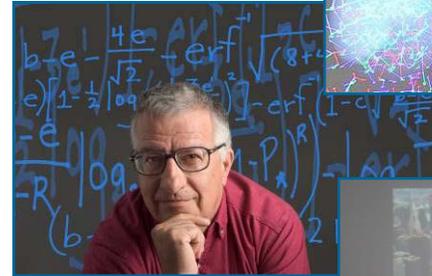
ITL Overview

To promote US innovation and industrial competitiveness by advancing

*measurement science,
standards, and
technology*

through research and development in

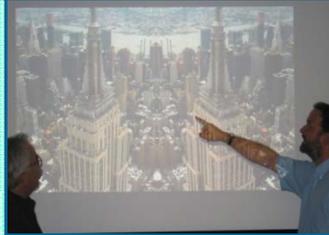
*information technology,
mathematics, and
statistics.*



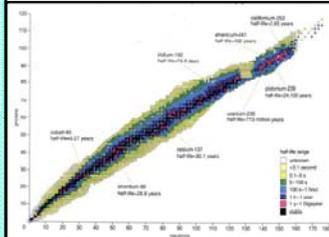


Core Competencies

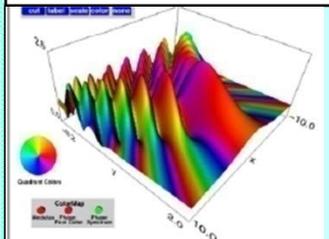
Technology Development



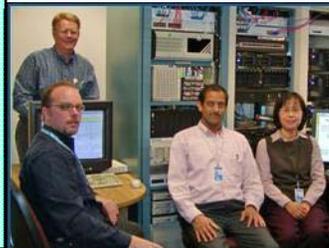
IT Measurement and Testing



Mathematical and Statistical Analyses for Measurement Science

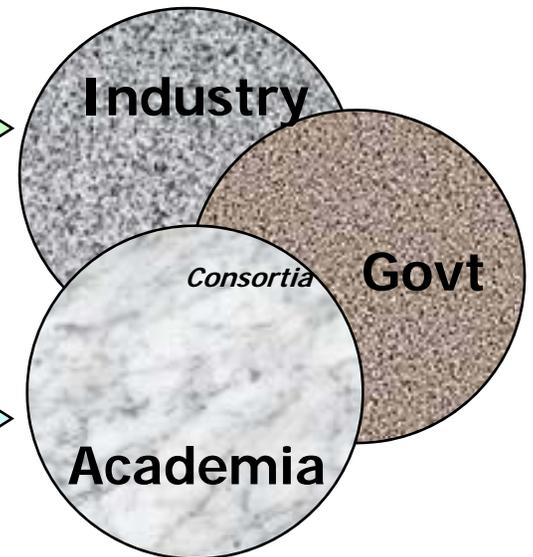


Modeling and Simulation for Measurement Science



IT Standards Development and Deployment

Customers





ITL Program Portfolio

- **Trust and Confidence in IT Systems and Applications**
 - Trustworthy Computing
 - Trustworthy Information Systems
 - Cyber and Network Security
 - Identity Management
- **Management and Exploitation of Data**
 - Information Discovery, Use, and Sharing
- **Future Information Systems**
 - Complex Systems
 - Pervasive Information Systems
- **IT in Science and Engineering**
 - Enabling Scientific Discovery
 - Virtual Measurement Systems



Trustworthy Information Systems Program

- **Foundational and applied research across a broad range of technologies and capabilities**
 - needed to improve security, assurance, and trust in computer-based systems and networks
 - supports national defense, national and homeland security, economic competitiveness, and other national priorities
- **Conduct Research & Development To:**
 - Provide solutions that advance trustworthy information system science and technology
 - Develop and exploit new methods, techniques, & technologies for building, testing, measuring and analyzing trustworthy information systems
 - Develop specifications, standards and guidance supporting development and evaluation of trustworthy information systems
 - Reduce cost and time of producing trustworthy information systems



ITL Assurance-Related Work Areas (in red)

- **Software Assurance, Metrics, & Test Method Research**
- **Voting System Security and Standards**
- **Security Testing, Metrics, & Standards**
- **Cyber Security & Internet Infrastructure Protection**
- **Biometrics Technology**
- **GRID Systems Reliability & Robustness**
- **Computer Forensics & Tool Testing**
- **Health Information Technology**
- **Human Language Translation**
- **Quantum Key Distribution Network**
- **Enabling Scientific Discovery**
- **Virtual Measurement Systems**
- **Combinatorial Testing**



ITL Projects to be Presented Today

- **“Measurement Framework for Software Assurance and Information Security”**
 - *Ron Ross, Peter Mell, ITL Computer Security Division*
- **Panel Discussion:**
 - FISMA Risk Management Framework
 - Security Content Application Protocol (SCAP) and its contributing data:
 - Common Vulnerability Enumeration (CVE)
 - Common Vulnerability Scoring System (CVSS)
 - Common Configuration Enumeration (CCE)
- The Common Configuration Scoring System (CCSS)



ITL Projects to be Presented Today

“Conventions for Software Facts”

– *Paul Black, ITL Software and Systems Division*

- **Presentation: What should a “fact sheet” for software consumers contain? Key questions include:**
 - Who is its audience?
 - What products should it cover?
 - What should it say about the software?



ITL Projects to be Presented Today

“A Model for Evaluation of Securing Risk in Enterprise Information Systems”

- *Anoop Singhal, ITL Computer Security Division*
- **Presentation: A metric for overall system risk requires:**
 - The capture of vulnerability interdependencies, (measuring security in the exact way that real attackers could penetrate the network)
 - Analysis of all attack paths through a network
 - A metric that is consistent, unambiguous, makes underlying assumptions explicit, and provides context for understanding security risk alternatives



ITL Projects to be Presented Tomorrow

“Software Assurance in the next Voluntary Voting System Guidelines (VVSG)”

– *John Wack, ITL Software and Systems Division*

• Presentation: The Voluntary Voting System Guidelines address the following areas:

- Core Requirements & Testing
- Human Factors and Privacy
- Security and Transparency



Other ITL Assurance-Related Projects

- **Software Assurance Metrics And Tool Evaluation (SAMATE) project**
 - Co-sponsored by ITL and DHS
 - Project began in 2004
- **SAMATE goals:**
 - Testing software assurance tools
 - Measuring the effectiveness of tools
 - Identifying gaps in software assurance tools and methods.
- **Current areas of concentration**
 - Source code security analyzers
 - Web application scanners
 - Tool effectiveness studies
 - Software tool test data
 - Automated test case generation



Other ITL Assurance-Related Projects

- **Automated Combinatorial Testing**
- **Goals: Reduce testing cost and improve cost-benefit ratio for software assurance testing**
 - Merges automated test generation with combinatorial methods.
 - Research shows software failures involve interaction of small number of variables (1 to 6)
 - Testing all t-way combinations for small t can be effective
 - New algorithms & faster processors make combinatorial testing practical
 - Huge increase in performance & scalability
 - Being studied for use in software assurance tool testing
- **Collaborators: University of Texas, UMBC, UNLV, GMU, SEI/CMU**
- **NIST software obtained by CISCO, Microsoft, Innovative Defense Technologies and others**



Other ITL Assurance-Related Projects

- **National Software Reference Library (NSRL)**
 - A repository of known software, file profiles, and file signatures for use by law enforcement and other organizations in computer forensics investigations
 - NSRL contains over 70 million software files and signatures
 - Library includes operating systems, database management systems, utilities, graphics images, component libraries, etc., in all their different versions.
 - NSRL contains both benign *and* malicious software, to be used as a filter of "known" file signatures, not necessarily "known good" file signatures
 - Investigators can search for files that are not what they appear to be (e.g., the file has the same name, size, and date as the original file, but not the same content)



NIST Publications

- **Some of NIST's Special Publications (available on your Forum CD)**
 - **SP 800-115:** DRAFT Technical Guide to Information Security Testing
 - **SP 800-83:** Guide to Malware Incident Prevention and Handling
 - **SP 800-95:** Guide to Secure Web Services
 - **SP 800-64:** DRAFT Security Considerations in the System Development Life Cycle
 - **SP 800-53:** Recommended Security Controls for Federal Information Systems
 - **SP 500-269:** Software Assurance Tools: Web Application Scanner Functional Specification Version 1.0
- **SAMATE Project (available on your SAMATE CD)**
 - Source Code Analysis Tool Tests
 - SAMATE Papers
 - Workshop proceedings



Many Ways to Partner with NIST

- Cooperative Agreements
- Patents/Licenses
- Consortia
- Guest Researcher Agreements
- Facility Use Agreements
- Post-doctoral Research Programs
- Grants
- Informal Collaborations
- Summer Undergraduate Research Fellowships (SURF)
- Workshops
- Other...



Massachusetts
Institute of
Technology



University of Colorado
at Boulder



Agilent Technologies



NIST
National Institute of Standards and Technology



Contact

- **Tom Rhodes - Manager, Trustworthy Information Systems Program**
 - (301) 975-3295
 - trhodes@nist.gov
- **Kirk Dohne – Director, Office of Programs**
 - (301) 975-8480
 - kirk.dohne@nist.gov
- **Cita M. Furlani – Director, ITL, NIST**
 - (301) 975-2900
 - cita.furlani@nist.gov
- **Web Sites:**
 - NIST: <http://www.nist.gov>
 - ITL: <http://www.itl.nist.gov>