The Computer Security Division

Measurement Science for IT  IT for Measurement Science
The Importance of Standards

Article I, Section 8: The Congress shall have the power to...fix the standard of weights and measures

- National Bureau of Standards established by Congress in 1901
- Eight different “authoritative” values for the gallon
- Electrical industry needed standards
- American instruments sent abroad for calibration
- Consumer products and construction materials uneven in quality and unreliable

Estimated that 80% of global merchandise trade is influenced by testing and other measurement-related requirements of regulations and standards
NIST Mission and Programs

“...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 Laboratories
- Create critical measurement solutions and promote equitable standards to stimulate innovation, foster industrial competitiveness, and improve the quality of life.

Hollings Manufacturing Extension Partnership
- Nationwide network of resources helping smaller manufacturers compete globally

Baldrige Performance Excellence Program
Promoting and recognizing performance excellence via information and Presidential awards in manufacturing, service, small business, education, health care, and the nonprofit sector

Technology Innovation Program
Supports development of cutting edge technologies by the private sector and universities to address critical national needs and key societal challenges

NIST is the nation’s innovation agency
NIST has... ...four joint institutes

JILA
NIST + University of Colorado

Institute for Bioscience and Biotechnology Research
NIST + University of Maryland
College Park + The University of Maryland Baltimore

Joint Quantum Institute
NIST + University of Maryland + NSA

Hollings Marine Laboratory
NIST + NOAA + South Carolina
+ College of Charleston
+ Medical University of South Carolina
NIST has... ... two main campuses

Gaithersburg, MD

Boulder, CO

Courtesy HDR Architecture, Inc./Steve Hall © Hedrich Blessing

© Geoffrey Wheeler
NIST Products and Services

Measurement Research
• ~ 2,200 publications per year

Standard Reference Data
• ~ 100 different types
• ~ 6,000 units sold per year
• ~ 226 million data downloads per year

Standard Reference Materials
• ~ 1,300 products available
• ~ 30,000 units sold per year

Calibration Tests
• ~ 18,000 tests per year

Laboratory Accreditation
• ~ 800 accreditations of testing and calibration labs
ITL Mission

ITL promotes innovation and industrial competitiveness through research and development at the intersection of measurement science and information technology.
Core Focus Areas

- Research, Development, Standards, Guidelines, Reference Materials
  - Security Mechanisms (e.g. protocols, cryptographic, access control, auditing/logging)
  - Security Mechanism Applications
    - Confidentiality
    - Integrity
    - Availability
    - Authentication
    - Non-Repudiation
    - Accessibility
    - Safety
- Secure System and Component configuration
- Conformance validation and assurance of security properties of products and systems
Delivery Mechanisms

1) Standards – FIPS, International Consensus, National Consensus
2) Guidelines – NIST SPs, IRs
3) Journal & Conference papers
4) Reference Materials
5) Workshops & Conferences – hosting and participation in
6) Consortia & Forums
7) Training
8) Reference Implementations & Demonstrations
9) Conformance Verification Activities
10) Test, Tools and other conformance determination tools
11) Standards Development Organization Participation
Community Engagement

- **Industry**
  - Accessing Expertise and Leveraging Resources
  - Coordinating Standards and Initiatives

- **Academia**
  - Accessing Expertise and Leveraging Resources
  - Representative Institutions and Consortia

- **International**
  - Formal Standards Groups
  - Accessing Expertise and Leveraging Resources

- **Federal, State, and Local Government**
  - Interdepartmental
  - Department of Commerce
  - State and Local Governments
Community Engagement Examples

- Chief Information Officers (CIO) Council
- Federal Systems Security Governance Board Member
- National Cyber Study Group (NCSG) Member
- Cyber Security and Information Assurance Interagency Working Group
- Information Security Research Council
- Common Terrorism Information Security Standards Working Group
- Committee for National Security Systems (Observer)
- Information Sharing Environment Enterprise Architecture Security Working Group
- Supply Chain Risk Management Working Group
- Federal Information Systems Security Educators' Association
- Software Assurance Forum
- IT Entrepreneurs' Forum
- Governance Coordinating Council
- Federal Enterprise Architecture Security and Privacy Profile Working Group
- Interagency C&A Transformation Working Group
- Internet Engineering Task Force (IETF) Security Chair
- International Organization for Standardization (Chair/Convener several Committees, Work Groups, and Task Forces)
- American National Standards Institute
- International Committee for Information Technology Standards (Biometrics Chair)
- Biometrics Consortium Co-Chair
- National Science & Technology Council Committee on Biometrics and Identity Management (Co-Chair)
NIST Responsibilities for Cybersecurity

• NIST is responsible for **developing standards and guidelines**, including minimum requirements, that provide adequate information security for all agency operations and assets in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002/2014, NIST Act, but such standards and guidelines shall not apply to national security systems.

• Under FISMA NIST shall **“conduct research,”** as needed, to determine the nature and extent of information security vulnerabilities and techniques for providing cost-effective information security.”

• NIST develops **guidelines consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Securing Agency Information Systems**, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

• In accordance with the Cyber Security Research and Development Act, The National Institute of Standards and Technology **develops, and revises as necessary, checklists setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system** that is, or is likely to become, widely used within the Federal Government.

• Homeland Security Presidential Directive 7; “The Department of Commerce will **work with private sector, research, academic, and government organizations to improve technology for cyber systems and promote other critical infrastructure efforts**, including using its authority under the Defense Production Act to assure the timely availability of industrial products, materials, and services to meet homeland security requirements.”

• Homeland Security Presidential Directive 12: “The Secretary of Commerce shall promulgate in accordance with applicable law a Federal **standard for secure and reliable forms of identification** (the "Standard")”
NIST Responsibilities for Cybersecurity

- Cloud Computing
  - America COMPETES Reauthorization Act of 2010
  - Federal Cloud Computing Strategy (February 2011)
- Healthcare
- Identity Management
  - National Strategy for Trusted Identities in Cyberspace
- Smart Grid
  - Energy Independence and Security Act (EISA) of 2007
- Voluntary Voting System Standards
  - Help America Vote Act
  - Military and Overseas Voter Empowerment (MOVE) Act of 2009
- Cyber Security Education
  - Lead for the National Initiative for Cyber Education (NICE)
Cryptography as Foundational To Secure Data

- Strong cryptography improves the security of systems and the information they process.
- Enhances the availability of secure applications for users to use
  - Cryptography
  - Public Key Infrastructure (PKI)
  - e-authentication.
Cryptographic Standards

- Block Ciphers
- Random Number Generation
- Digital Signatures
- Key Agreement & Transport
- Key Management
- Advanced Hash Algorithm Competition
- Hash Algorithms
Cryptographic Algorithms

Algorithms authorized for use by the US Civilian Agencies are specified in

- FIPS 186-4 Secure Hash Standards
- FIPS 197 Advanced Encryption Standard
- FIPS 198-1 Keyed Hash Message Authentication Code
Key Management (SP 800-57)

• Key Establishment Schemes
  – Key Agreement Schemes
  – Key Transports
  – Key Wrapping
  – Key Confirmations
  – Random Number Generation

• Key Life spans (crypto periods)
• Public/Private Keys
  – Key Validation
  – Key Revocation
FIPS-Validated Cryptographic Modules

- Cryptographic modules *may* be embedded in other products
  - Applicable to hardware, software, and firmware cryptographic modules
  - Must use the validated version and configuration
  - e.g. software applications, cryptographic toolkits, postage metering devices, radio encryption modules

- Does **not** require the validation of the larger product
  - Larger product is deemed compliant to requirements of FIPS 140-2
Cryptographic Testing

• Cryptographic Modules Surveyed (during testing)
  – 48.8% Security Flaws discovered
  – 96.3% FIPS Interpretation and Documentation Errors

• Algorithm Validations (during testing) (DES, Triple-DES, DSA and SHA-1)
  – 8.5% Security Flaws
  – 65.1% FIPS Interpretation and Documentation Errors

• Areas of Greatest Difficulty
  – Physical Security
  – Self Tests
  – Random Number Generation
  – Key Management
Cryptographic Research

- Cryptography in Constrained Environments
- Stream Ciphers
- Privacy-Enhanced Cryptographic Mechanisms
- Post-Quantum Cryptography
- Rabin Beacon
- New Elliptical Curves