

# Computer Security Division

Information Technology Laboratory

National Institute of Standards and Technology

September 14, 2006

# NIST Information Technology Laboratory Computer Security Division

## Mission (What is the problem to be solved?)

- Provide standards and technology to protect information systems against threats to the confidentiality of information, integrity of information and processes, and availability of information and services in order to:
- Build trust and confidence in Information Technology (IT) systems.

# Threats (What is the problem?)

- Intrusion via publicly accessible portals
  - Directly disrupt system operations (e.g., flooding attacks that dramatically slow system access and applications)
  - Defeating identification, authorization, and access control mechanisms to:
    - Implant disruptive or destructive code viruses, worms, and spyware
    - Access privileged or private data (e.g., unclassified but sensitive data; personally identifiable information; passwords, keys, and other data that grants access to other sensitive or critical information or processes)
- Physical access to/intrusion into IT components\*
- Analysis and defeat of protection mechanisms that permits intrusion into IT components or interpretation and exploitation of information processed by or exchanged among IT components.\*

\* Consequences similar to intrusion via publicly accessible portals

# Challenges (Why is it hard?)

- Complexity of IT systems (Hardware complexity compounded by software complexity and diversity; complexity compounded also by data inputs associated with Turing machines and combining individual systems into computing grids; networks and global inter-networks)
- Interdependence of systems to be protected (Further compounding of complexity; unintended consequences of incorporating security measures into system structure, operation, and management)
- Diversity of threat sources (Individuals, criminal enterprises, terrorist organizations, nation states)
- Continually evolving threat environment
- Operational and cost impact of security controls
- Diversity of community supported
  - Standards and guidelines mandatory for Federal departments and agencies (Cost consequences to customer community)
  - Voluntary use of standards and guidelines by others (Potentially ineffective, or even harmful, partial implementation of controls)

# CSD Security Responses

- Encryption of information in storage and/or in transit
- Use of cryptographic processes to provide confidence in the source and content of information
- Multi-factor identification for access control
- Cryptographic mechanisms to support user authentication (e.g., digital signature, authentication codes)
- Enforcement of domain separation and access control policies in system components Establishment of technical, operational, and management requirements for systems
- Methods for determination of conformance of systems to security requirements

# Key Concepts

- Engage private sector to supplement technical expertise, foster feasibility, and maximize utility of NIST security standards and technology.
- Employ operational and management controls to mitigate limitations of current security technology
- Employ technical controls as practical to minimize the costs of labor-intensive operational and management controls

# Impact (Who cares?)

- Congress (Conformance to legislative mandates)
- Executive Office of the President
  - System owner impacts
  - Conformance to Presidential Directives, Executive Orders, and OMB Memoranda/Circulars
  - Cost reductions due to enabling of automated services (e.g., telecommuting, e-Government)

# Impact (Who cares?)

- System owners (Public Sector and Private Sector)
  - Reduction of losses due to maliciously induced service disruptions (Both IT services and infrastructures and other critical national infrastructure accessible via IT services or to which IT services are a critical protection or operational component)
  - Reduction of liability, operational effectiveness, and other consequences of confidentiality/privacy breaches
  - Reduction of losses due to data manipulation
    - Fraud
    - Privileges permitting service disruption or confidentiality/privacy breach
  - Additional service offerings enabled by increased confidence resulting from improved IT system security (e.g., e-Commerce, e-Government)

# Major FY07 Activities

- Key Initiatives
  - Secure Hash
  - Security Metrics
  - Security Product Assessment Requirements and Methods
- Security support to ITL and other NIST programs
  - Voting
  - Health Care
  - SIGs
    - Identity Management
    - Other
- Maintenance of existing body of standards and guidelines in response to evolution of threat technologies and institutional environments
- General technical support to requests from OMB and other EOP organizations, GAO and Congressional staff, individual Departments and Agencies, other DoC organizations, and other NIST organizations.

# Division Structure

(How is the division organized for FY07?)

- **Division Office**
  - Overall division management
  - Coordination of support to ITL programs
  - 4 Federal employees
- **Security Technology**
  - Security mechanisms' development, standards, and guidelines
  - 20 Federal employees
- **Security Research and Emerging Technologies**
  - Security applications research and guidelines
  - 23 Federal employees
- **Security Management and Guidance**
  - Security Management standards, guidelines, and outreach
  - 17 Federal employees
- **Security Testing and Metrics**
  - Cryptographic algorithm module validation program management
  - 10 Federal employees

# IT Security Mechanisms

**Goal:** Develop and improve mechanisms to protect the integrity, confidentiality, and authenticity of Federal agency information by developing security mechanisms, standards, testing methods, and support infrastructure requirements and methods.

## **Programs:**

- Security Mechanism Standards Toolkits
  - Cryptographic Standards
  - Password Mechanisms
- Cryptographic Key Infrastructures
- Develop measures of effectiveness
- Applications Support
  - E-Authentication
  - Voting Systems (with SDCT)

**FY06 Staff:** 20 Employees, 2 Students, 7 Guest Researchers

## **Basis for Program Priority:**

- PITAC Cyber Security Report lists authentication technologies at top of R&D priority list (2/05).
- NIST FY 2007 Budget Request cites encryption standards technical expertise and response to statutory assignments as having saved industry \$1 billion (2/06).
- CSIA *Federal Plan for Cyber Security and Information Assurance R&D* lists authentication and cryptography among its top funding priorities (4/06).

**FY07 Priorities:** Secure Hashing Algorithm replacement research, Password Guideline Revision, E-Authentication and Key Management Guidelines

**Products:** Federal Information Processing Standards, NIST Special Publications (SPs), ANSI & INCITS Standards, ISO/IEC Standards, IEEE Standards, IETF RFCs.

Security Research and Emerging Technologies Group

# IT Security Research and Applications

## Goal:

Devise advanced security methods, tools, and guidance through conducting near and midterm security research

## Programs:

- Security Research
  - Access Control and Policy Management
  - Forensics
  - Ad hoc Networks and Wireless Security
  - Combinatorial Testing (Pseudo exhaustive)
  - Quantum Crypto Protocols
- National Vulnerability Database
- Security Related Protocol Standards.
- Identity Management (PIV, Smart Cards and Biometrics)
- OS and Apps Security Hardening Standards
- Technical Guidance for Federal Agencies

**FY06 Staff:** 23 Employees, 2 Students, 4 Guest Researchers

## Basis for Program Priority:

- Research, modeling, and reference implementation builds vital competencies
- FISMA and prior legislation directs NIST to conduct research in support of its national role of providing security standards and guidance to Fed Agencies.
- CSIA *Federal Plan for Cyber Security and Information Assurance R&D* lists Access Control and Privilege Management as a top national priority (4/06).
- HSPD-12 drove the most resource intensive FY06 activities.

**FY07 Priorities:** Security metrics program initiation, applications and configuration guidelines, wireless security, security in quantum computing environments, electronic identity standards and guidelines.

**Products:** FIPS, NIST SPs, Formal Security Models, Open Software, Reference & Prototype Implementations, Journal & Conf. Papers, ANSI & INCITS Standards, IETF RFCs, Patents.

# IT Security Management

## **Goal:**

Provide computer security guidance to ensure sensitive government information technology systems and networks are sufficiently secure to meet the needs of government agencies and the general public.

## **Programs:**

- FISMA Implementation Project
  - Security Standards and Guidelines
- Division Outreach
  - Computer Security Resource Center
  - Federal and Private sector Practices web site (FASP/PPSP)
  - Small Business Outreach
- Return on Security Investment Trade-offs
- Facilitate exchange of security information among Federal government agencies and private sector
  - Federal Computer Security Program Managers Forum
  - Information Security and Privacy Advisory Board
  - Federal Information Systems Security Educators' Association (FISSEA)

**FY06 Staff:** 17 Employees

## **Basis for Program Priority:**

- The FISMA Implementation Project was established in January 2003 to produce security standards and guidelines required by FISMA.
- Cyber Security: Innovative Technologies for National Security are identified in the Research Initiatives for President's Innovation Agenda
- The Information Security and Privacy Advisory Board founded in accordance with 15 U.S.C. 278g-4, pursuant to the Federal Advisory Committee Act, 5 U.S.C.
- Appendix III to OMB Circular No. A-130 charges the Secretary of Commerce to develop and issue appropriate standards and guidance for the security of sensitive information in Federal computer systems.

**FY07 Priorities:** FISMA implementation guidelines and support, product security assessment requirements development, return on security investment determination.

**Products:** Federal Information Processing Standards, NIST Special Publications

# Cryptographic Testing & Validation

## Goal:

Improve the security and technical quality of cryptographic products needed by Federal agencies (U.S., Canada, and UK) and industry, by developing standards, test methods & validation criteria, and the accreditation of independent third party testing laboratories.

## Programs:

- Cryptographic Module Validation Program (CMVP)
- Cryptographic Algorithm Validation Program (CAVP)
- Test tools and algorithm & protocol test suite development
- Cryptographic Module Testing Laboratory and Personal Identification Verification laboratory accreditation
- Security Testing Research

FY06 Staff: 10 Employees

## Basis for Program Priority:

- NIST FY 2007 Budget Request cites encryption standards technical expertise and response to statutory assignments as having saved industry \$1 billion (2/06).
- CSIA *Federal Plan for Cyber Security and Information Assurance R&D* lists authentication and cryptography among its top funding priorities (4/06).
- ISO19790: Security Requirements for Cryptographic Modules accepted as an international standard (5/06)

FY07 Priorities: FIPS 140-3 publication, maintain effectiveness of cryptographic algorithm and module validation programs, incorporate NIST personal identity verification program test validation, establish basis to support future NVLAP-based product assessment validation activities.

Products: FIPS 140-2, ISO Standards, Implementation Guidance, cryptographic module and algorithm validation, laboratory accreditation, test tools, algorithm & protocol test suites

# Computer Security Division Resources

- 73 Federal employees (65 Professional Staff)
- 60% of professional staff with graduate degrees
- 25% of professional staff with PhDs

# FY06 Formal NIST Publications

- Special Publication 800-68: *Guidance for Securing Microsoft Windows XP Systems for IT Profession: A NIST Security Configuration Checklist*, October 2005
- Special Publication 800-87: *Codes for the Identification of Federal and Federally-Assisted Organizations*, October 2005
- NISTIR 7250: *Cell Phone Forensic Tools: An Overview and Analysis*," October 2005
- Special Publication 800-40 Version 2, *Creating a Patch and Vulnerability Management Program*, November 2005
- Special Publication 800-83: *Guide to Malware Incident Prevention and Handling*, November 2005
- Special Publication 800-21-1 Second Edition: *Guideline for Implementing Cryptography in the Federal Government*, December 2005
- Special Publication 800-77: *Guide to IPsec Virtual Private Networks*, December 2005
- NISTIR 7275: "Specification for the Extensible Configuration Checklist Description Format (XCCDF)," January 2006
- NISTIR 7284: "Personal Identity Verification Card Management Report", January 2006
- NISTIR 7285"Computer Security Division - 2005 Annual Report", February 2006
- Special Publication 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006
- Special Publication 800-76: *Biometric Data Specification for Personal Identity Verification*, February 2006

# FY06 Formal NIST Publications (Continued)

- Special Publication 800-56A: *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2006
- Special Publication 800-73 Revision 1: *Interfaces for Personal Identity Verification*, March 2006
- FIPS 200: *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
- NISTIR 7290: "Fingerprint Identification and Mobile Handheld Devices: An Overview and Implementation", March 2006
- Special Publication 800-63 (Version 1.0.2 ): *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology*, April 2006
- Special Publication 800-85A: *PIV Card Application and Middleware Interface Test Guidelines* (Special Publication 800-73 compliance), April 2006
- NISTIR 7298: "Glossary of Key Information Security Terms," May 2006
- FIPS 201-1: *Personal Identity Verification (PIV) of Federal Employees and Contractors*, Updated June 2006
- Special Publication 800-90: *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, June 2006
- Special Publication 800-85B: *PIV Data Model Conformance Test Guidelines*, July 2006
- NISTIR: "Personal Identity Verification Demonstration Summary," August 2006
- Published Drafts [Public Review]: 16 Special Publications (plus two FIPS revisions in progress)

# Thank you!

William C. Barker

[wbarker@nist.gov](mailto:wbarker@nist.gov)

301-975-8443

<http://csrc.nist.gov>