Information Technology Laboratory

Computer Security Activities Status

National Institute of Standards and Technology

June 7, 2007

NIST Information Technology Laboratory
Computer Security Division

Mission (What is the institutional goal?)

- 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 (Problems being addressed?)

- Intrusion via publicly accessible portals
  - Directly disrupt system operations (e.g., flooding attacks that dramatically slow system access and applications)
  - Compromising 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)

NIST 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)
- Industry (Enabling secure and reliable electronic commerce)
- Citizens (Privacy protection)

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 IT
  - ITL Program Initiatives
    - Support Identity Management Program
    - Help establish other programs (e.g., Cyber Security, Trustworthy Networking, Trustworthy Software)
- Maintenance of existing body of standards and guidelines in response to evolution of threat technologies and institutional environments
- Integrate support to national and international standards bodies (e.g., ANSI, ISO, IEEE, IAB/IETF, ICAO)
- 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 (e.g., CNSS, TWIC, WHTI, E-Passport, REAL ID).

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)

FY07 Staff: 18 Employees, 5 Guest Researchers

Basis for Program Priority:

•Help America Vote Act (10/02)

•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 Hash 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 guidelines through conducting near and midterm security research.

Programs:

- Security Research
  - Access Control and Policy Management
  - Automation Assistance to FISMA Reporting (Security Content Automation)
  - Ad hoc Networks and Wireless Security
  - Combinatorial Testing (Pseudo exhaustive)
  - Quantum Crypto Protocols
- National Vulnerability Database
- Protection of Personally Identifiable Information (PII)
- Security Related Protocol Standards.
- Identity Management (PIV, Smart Cards and Biometrics)
- Operating Systems and Applications Security Hardening Guidelines
- Technical Guidelines for Federal Agencies

FY07 Staff: 20 Employees, 1 Student, 6 Guest Researchers

Basis for Program Priority:

- Research, modeling, and reference implementation builds vital competencies
- FISMA, Cyber Security R&D Act, and prior legislation directs NIST to conduct research in support of its national role of providing security standards and guidelines to Federal Agencies (12/02).
- PITAC Cyber Security Report (2/05)
- 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-7 and HSPD-12 are driving the most resource intensive FY07 activities.

FY07 Priorities: Security metrics program initiation, security configuration guidelines, wireless security, secure use of RFIDs, security in quantum computing environments, electronic identity standards and guidelines.

Products: FIPS, NIST Special Pubs, Formal Security Models, Open Software, Reference & Prototype Implementations, Journal and Conference Papers, ANSI & INCITS Standards, IETF RFCs, Patents.

Security Management and Assistance Group

IT Security Management

Goal:

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

Programs:

- Standards and Guidelines
- Outreach
- Additional Initiatives

FY07 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.

Basis for Program Priority (continued):

- 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 guidelines for the security of sensitive information in Federal computer systems.

FY07 Priorities: FISMA implementation guidelines and support, product security assessment requirements development, update of guideline documents.

Products: Federal Information Processing Standards, NIST Special Publications, NIST Interagency Reports.

Security Testing and Metrics Group

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

FY07 Staff: 9 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 Guidelines, cryptographic module and algorithm validation, laboratory accreditation, test tools, algorithm & protocol test suites

FY07 NIST Publications

- Special Publication 800-100: *Information Security Handbook: A Guide for Managers,* October 2006
- Draft Special Publication 800-103: *An Ontology of Identity Credentials, Part 1: Background and Formulation,* October 2006
- Special Publication 800-89: *Recommendation for Obtaining Assurances for Digital Signature Applications,* November 2006
- Special Publication 800-53 Rev 1*: Recommended Security Controls for Federal Information Systems,* December 2006
- Special Publication 800-76-1: *Biometric Data Specification for Personal Identity Verification,* January 2007
- Draft Special Publication 800-104: *A Scheme for PIV Visual Card Topography,* January 2007
- NISTIR 7358: *Program Review for Information Security Management Assistance (PRISMA),* January 2007
- NISTIR 7359: *Information Security Guide for Government Executives,* January 2007
- Special Publication 800-45 Ver 2: *Guidelines on Electronic Mail Security,* February 2007
- Special Publication 800-94: *Guide to Intrusion Detection and Prevention Systems (IDPS),* February 2007
- Special Publication 800-97: *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i,* February 2007
- Special Publication 800-98: *Guidelines for Securing Radio Frequency Identification (RFID) Systems,* April 2007
- NISTIR 7399: *Computer Security Division – 2006 Annual Report,* April 2007
- Special Publication 800-101: *Guidelines on Cell Phone Forensics,* May 2007
- Draft Special Publication 800-44 Ver 2: *Guidelines on Securing Public Web Servers,* May 2007
- Draft Special Publication 800-53A: *Guide for Assessing the Security Controls in Federal Information Systems,* May 2007
- *NISTIR 7275 Rev 2: Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.1.3,* May 2007
- NISTIR 7387, *Cell Phone Forensic Tools: An Overview and Analysis Update*, June 2007
- Special Publication 800-95: *Guide to Secure Web Services,* June 2007
- Draft Special Publication 800-53A: *Guide for Assessing the Security Controls in Federal Information Systems*, June 2007
- Draft Special Publication 800-44 Version 2, *Guidelines on Securing Public Web Servers*, June 2007
- Draft Special Publication 800-46 Version, *User's Guide to Securing External Devices for Telework and Remote Access*, June 2007

FY07 Formal NIST Publications (Continued)

- Special Publication 101, *Guidelines on Cell Phone Forensics*, June 2007
- Draft Special Publication 800-82 (Second Public Comment): *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security,* June 2007
- Draft Special Publication 800-111: *Guide to Storage Encryption Technologies for End User Devices,* June 2007
- Draft Special Publication 800-xx: *Guide to Protecting Personally Identifiable Information,* June 2007
- Draft Special Publication 800-xx: *Guide to SSL VPNs,* June 2007
- Draft Special Publication 800-41 Ver 2: *Guidelines on Firewalls and Firewall Policy,* July 2007
- Draft Special Publication 800-48 Ver 2: *Wireless Network Security: IEEE 802.11a/b/g/n, Bluetooth, and Other Technologies,* July 2007
- Draft Special Publication 800-70 Ver 2: *NIST National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*, July 2007
- Draft Special Publication 800-99: *Guide to Information Technology Security Standards and Guidelines,* July 2007
- Draft Special Publication 800-110: *FISMA Reference Model,* July 2007
- *NISTIR xxxx: Guide to the Common Vulnerability Scoring System (CVSS) Version 2.0,* August 2007
- Draft Special Publication 800-28 Ver 2: *Guidelines on Active Content and Mobile Code,* August 2007
- Draft Special Publication 800-xx: *The Security Content Automation Protocol (SCAP),* August 2007
- Draft Special Publication 800-xx: *The Information Security Automation Program (ISAP),* August 2007
- Draft Special Publication 800-xx: *Guide to Storage Encryption Technologies for Enterprises,* August 2007
- Draft Special Publication 800-42 Ver 2: *Technical Guide to Information Security Testing,* September 2007
- Draft Special Publication 800-30 Rev 1*: Risk Assessment for Information Technology Systems,* September 2007

Guide for Assessing the Security Controls in Federal Information Systems: *Building Effective Security Assessment Plans*

- Companion to SP 800-53, Revision 1
- Contains comprehensive catalog of assessment procedures matched to security controls in SP 800-53
- Third public draft significantly changed from second public draft
- How to: build and execute a *security assessment plan* to *assess* the controls in an information system
- Allows cost-effective, flexible, consistent assessments during information System:
  - Development and integration (e.g., system integrators)
  - Security implementation and operation (e.g., ISSOs)
  - Security management and oversight (e.g., authorizing officials)
  - Security assessment and monitoring (e.g., auditors, IGs)
- Makes compliance with FISMA easier & more efficient
- Expect incorporation into automated information security support tools

Some ITL Programs with Security Content

- Identity Management
- Cybersecurity
- Trustworthy Networking
- Trustworthy Software