Information Technology Laboratory

Computer Security Division

Donna F Dodson
National Institute of Standards and Technology
September 4, 2008

NIST Information Technology Laboratory
Computer Security Division

Mission

- 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.

Information Technology Laboratory
Cita Furlani, Director

Deputy Director
Jim St. Pierre

Office of the Assistant Director for Boulder
Brad Alpert, Actg.

Executive Office
Kendra Cole, Senior Management Advisor

Office of the Associate Director for Federal and Industrial Relations
Kamie Roberts

Office of Programs
Kirk Dohne

- **Complex Systems** — Sandy Ressler
- **Identity Management** — Jim Dray
- **Information Discovery, Use and Sharing** — Mary Brady
- **Enabling Scientific Discovery** — Tony Kearsley
- **Pervasive Information Technology** — Kamran Sayrafian
- **Virtual Measurements** — Andrew Dienstfrey
- **Cyber and Network Security** — Tim Grance
- **Trustworthy Information Systems** — Tom Rhodes

- **Mathematical and Computational Sciences** — Ron Boisvert
- **Advanced Network Technologies** — David Su
- **Computer Security** — Curt Barker
- **Information Access** — Marty Herman
- **Software and Systems** — Mark Skall
- **Statistical Engineering** — Antonio Possolo

Division Structure

- Division Office
  - Overall division management
  - Coordination of support to ITL programs
  - 4 Federal employees
- Security Technology
  - Security mechanisms' development, standards, and guidelines
  - 18 Federal employees, 3 Guest Researchers
- System and Networks Security
  - Security applications research, security guidelines, security checklists
  - 25 Federal employees, 3 Guest Researchers
- Security Management and Assistance
  - Security Management standards, guidelines, and outreach
  - 16 Federal employees
- Security Testing and Metrics
  - Cryptographic algorithm module validation program management
  - 11 Federal employees, 1 Guest Researcher
- ***Information Technology Lab Program Area Leadership***
  - Identity Management
  - Cyber and Network Security

Security Technology Group

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

FY08 Staff: 18 Employees, 3 Guest Researchers

FY08 Priorities:

Secure Hash Algorithm Competition,
Voting Security,
Key Management,
Cryptographic Algorithms,
IETF Security Management,
Identity Based Encryption,
Post-Quantum Cryptographic,
Cryptographic Protocols,
E-Authentication,
Key Management Guidelines.

Products:

Federal Information Processing Standards,
NIST Special Publications (SPs),
ANSI & INCITS Standards,
IEEE Standards,
IETF RFCs.

Security Technology Group Highlights

- Identity Based Encryption Workshop
- Galois Counter Mode for Authenticated Encryption
- SHA-3 Competition
- IETF PKIX Certificate Profile
- Hashed Based Message Authentication Code
- EAC Draft Voluntary Voting System Guidelines Test Suite

Systems and Network Security 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)
- National Vulnerability Database
- Protection of Personally Identifiable Information (PII)
- Security Related Protocol Standards
- Operating Systems and Applications Security Hardening Guidelines
- Technical Guidelines for Federal Agencies

FY08 Staff: 25 Employees, 3 Guest Researchers

FY08 Priorities:

Security Content Automated Protocol,
Policy Machine,
Automated Combinatorial Testing,
Standardizing Metrology for Information Security,
Security Configuration Guidelines,
Identity Management,
Biometric Interoperability,
Wireless Security.

Products:

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

System and Network Security Group Highlights

Research and Development and Cross Group/Program/Lab Activities

- **DNS/BGP/IPv6**
- **Policy Machine**
- **Combinatorial Testing**
- **Security Content Automation**
- **Identity Management Standards and Metrics**
- **Identity Systems Research**
- **Biometrics Interoperability**
- **Global eID**

Security Management and Assistance Group

IT Security Management

Goal:

Provide leadership, expertise, outreach, standards and guidelines in order to assist the federal IT community in protecting its information and information systems in order to allow our customers to rely on critical IT assets to accomplish their missions.

Programs:

- FISMA Standards and Guidelines
- Health Sector Security Support
- Outreach, Awareness and Training
  - Computer Security Resource Center (CSRC)
  - Federal and Private sector Practices web site (Federal Agency Security Practices and Public/Private Security Practices)
  - Small Business Outreach
  - Federal Computer Security Program Managers Forum
  - Information Security and Privacy Advisory Board (ISPAB)
  - Federal Information Systems Security Educators' Association (FISSEA)
- SDO Activities and Participation
  - ISO, ANSI, HIT-SP, DHS-ISS LOB, NTIA, CNSS, FEA, NCSA

FY08 Staff: 16 Employees

FY08 Priorities:

FISMA Implementation Guidelines and Support,
Security Assessment Provider Assessment,
Product Security Assessment Requirements development,
HealthIT Security support,
Security Outreach.

Products:

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

Security Management and Assistance Group Highlights

Research and Development and Cross Group/Program/Lab Activities

- Product Assurance Research With Cyber Security Program
- HAVA Risk Assessment Support to Group .01
- Attack Graph Research With Group .02
- S-CAP Mapping to FISMA With Group .02
- HIPAA Technical Control S-CAP Automation Mapping With Group .02
- Laboratory Accreditation Research for FISMA Products With Group .04
- Assist Security Test and Conformance Division With Nation Wide Health Information Network (NHIN) Security Requirements Validation
- Assist EEEL With Specific Areas of The Electric Independence and Security Act
- IDMS Metric Research With Identity Management Program
- FISMA (Previously updated)

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

FY08 Staff: 11 Employees

FY08 Priorities:

FIPS 140-3 Comment Resolution,

Maintain Cryptographic Algorithm and Module Validation Programs,

Accreditation of New Labs,

Incorporate new tests for key establishment.

Products:

FIPS 140-2,

ISO Standards,

Implementation Guidelines,

Cryptographic module and algorithm validation, laboratory accreditation, test tools, algorithm & protocol test suites.

Security Testing and Metrics Group Highlights

- Continued growth in the number of cryptographic modules validated
- Over 120 validations in 2008 (to date)
- All four security levels of FIPS 140-2 represented on the Validated Modules list
- Over 245 participating vendors

CSD Supported Workshops

- HIPAA Security Rule Implementation and Assurance Workshop
- Federal Desktop Core Configuration Implementers Workshop
- Federal Computer Security Program Managers' Forum January 2008 Meeting
- Idtrust 2008
- Federal Information Systems Security Educators' Association (FISSEA) Annual Conference
- FIPS 140-3: Software Security Workshop
- Federal Computer Security Program Managers' Forum March 2008 Meeting
- PIV PACS Integration Workshop
- Federal Computer Security Program Managers' Forum Annual Offsite

CSD Supported Workshops (Cont)

- Identity Based Encryption Workshop
- Computer Security Testing Laboratory Managers Meeting
- Federal Computer Security Program Manager's Forum August Meeting
- Biometric Consortium Conference 2008
- 2008 Security Automation Conference and Workshop