NIST Laboratory Research Program Contributions to Cybersecurity Standards

Donna F. Dodson
Deputy Chief Cybersecurity Advisor
Information Technology Laboratory
National Institute of Standards and Technology
October 14, 2009

ITL's Mission…

- … is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics.

Why Research?

- While Standards has always been in our name, research has always been an integral part of our method.
  - Research advances science.
  - Research informs our standards and metrics development activities.
  - Research establishes new technologies, creating opportunities.

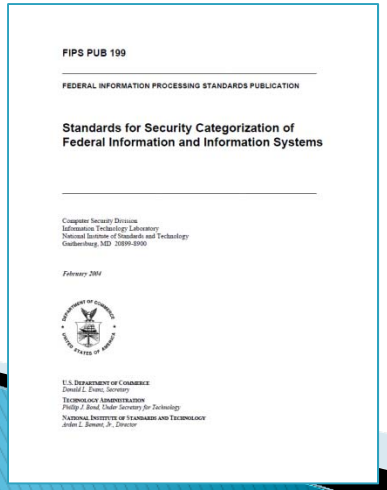
NIST Cybersecurity Research Areas

- Authorization
- Biometrics
- Cryptography
- Forensics
- Identification & Authentication
- Key Management
- Network Security
- Product Assurance
- Security Metrics

- Security Automation
- Security for Emerging Technologies
- Security for Sector-Specific Applications
- Trustworthy Software
- Usability

NIST Cybersecurity Standards Activities

- Technical Leadership in Standards Development Organizations
  - ANSI INCITS, ISO, ITU-T, IETF, IEEE
  - Sector-specific organizations: HL7, IHE, ATA, BioAPI Consortium, W3C
- NIST Federal Information Processing Standards (FIPS)
- Security Guidelines and Best Practices
  - NIST Special Publications and Interagency Reports


FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

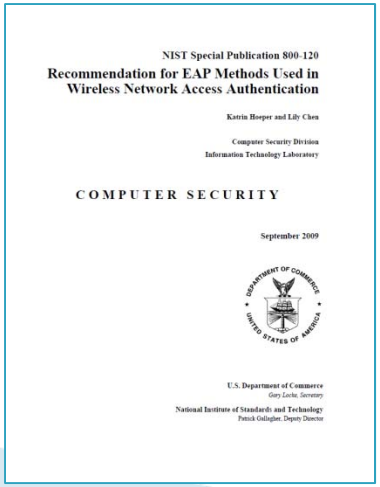
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

February 2004

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director


NIST Special Publication 800-120

Recommendation for EAP Methods Used in Wireless Network Access Authentication

Katrin Hoeper and Lily Chen

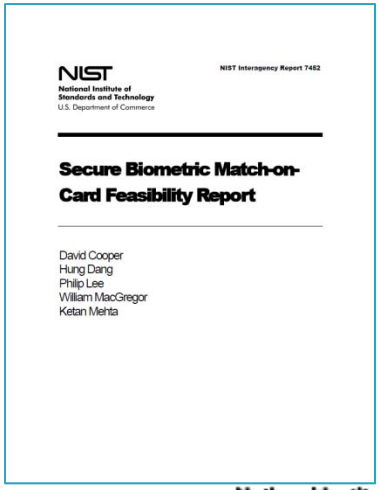
Computer Security Division
Information Technology Laboratory

COMPUTER SECURITY

September 2009

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick Gallagher, Deputy Director


NIST Interagency Report 7452

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

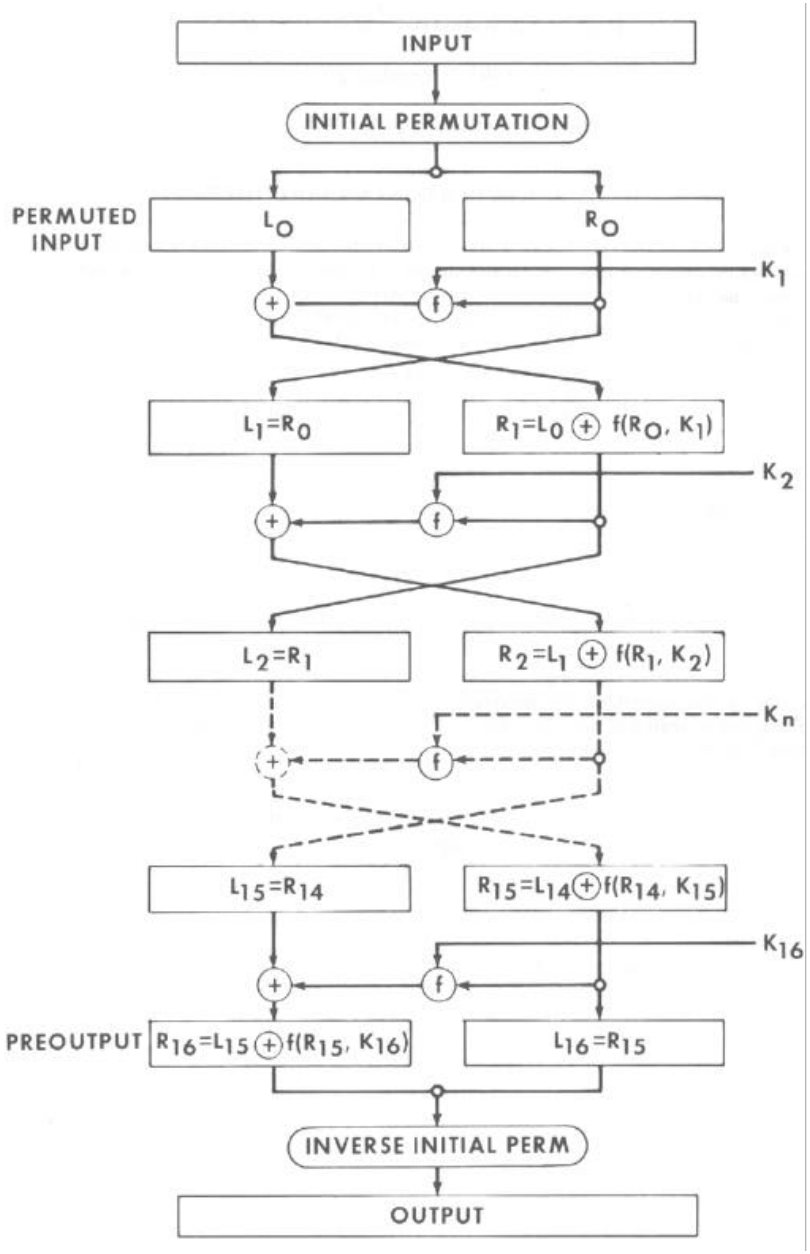
Secure Biometric Match-on-Card Feasibility Report

David Cooper
Hung Dang
Philip Lee
William MacGregor
Ketan Mehta

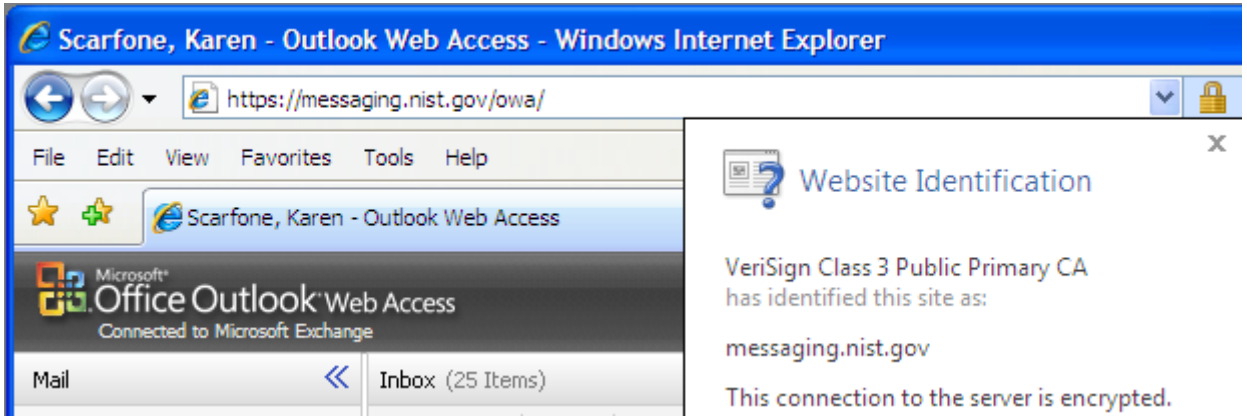
Improving Cybersecurity Through Research and Standards: A Case Study

Cryptography

- Data Encryption Standard (DES)– The Pioneer
  - FIPS 46, *Data Encryption Standard* was the first unclassified, publicly disclosed algorithm standard for the protection of U.S. government sensitive, unclassified information
  - Adopted by ANSI, ISO/IEC (TDEA)
  - World's most widely used encryption algorithm, particularly to protect financial information, for 25 years
- Related Research
  - Generated open research and development in cryptanalysis (esp. block ciphers), cryptographic testing, and key management

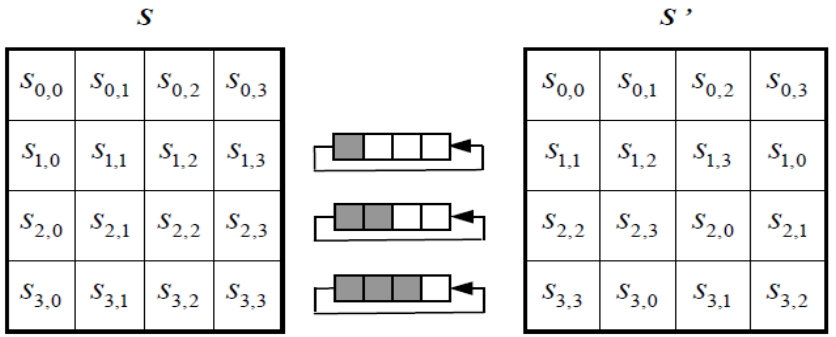


Cryptography in daily life

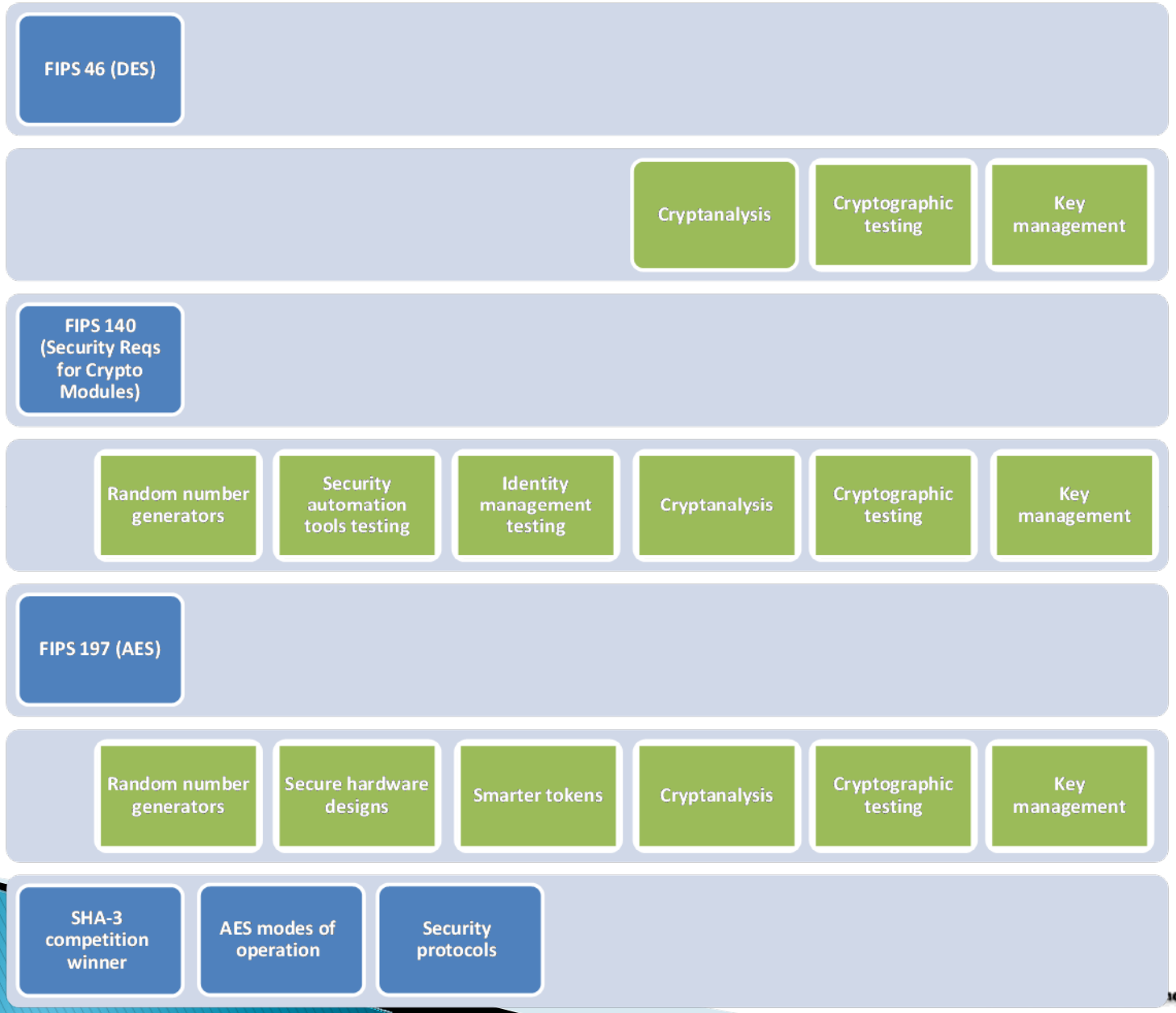


Cryptography

- Advanced Encryption Standard (AES)
  - NIST, through an open and transparent process, sponsored the first International Cryptographic Algorithm Design Competition
  - Innovative design criteria included support for various PC hardware architectures, software, and smart cards
  - Fifteen submitted designs; investigations and analysis published by cryptographers at NIST and around the world
  - NIST selected Rijndael and specified the algorithm in FIPS 197, *Advanced Encryption Standard*
  - Adopted by standards bodies and the IT vendor community; NSA announced use of AES to protect national security systems
- Related Research
  - Generated new research in cryptanalysis, smarter tokens, and security hardware designs

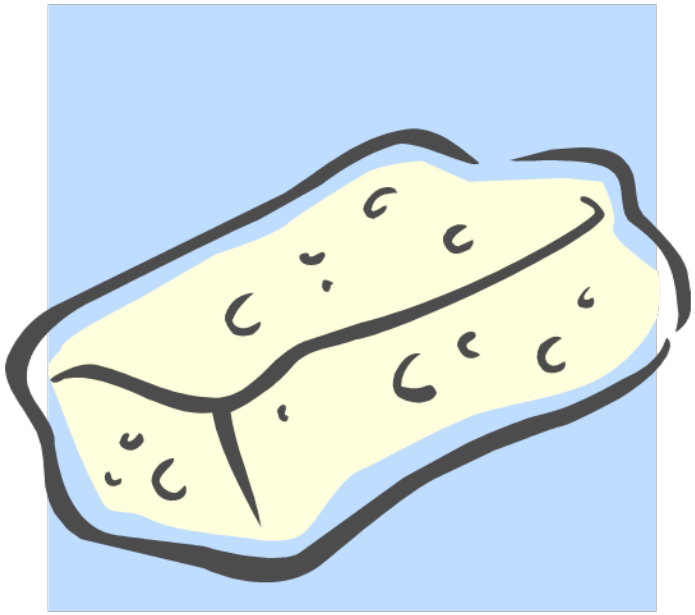


Examples from the cycles of research and standards for cryptographic algorithms



Cryptography

- Secure Hash Algorithm 3 (SHA-3) – In progress
  - Cryptanalytic attacks on several cryptographic hash algorithms
  - Cryptographic community encouraged NIST to sponsor a Cryptographic Hash Competition
  - Design criteria that advance the state of the art: performance; drop-in compatibility; and security
  - Over 60 entries submitted from around the world
  - NIST recently selected 14 to advance to round 2



Brief Summary of NIST Research Contributions to Crypto Standards

- Publication of NIST standards for cryptographic algorithms creates research opportunities
  - PKI and Symmetric Key Management
  - Smart Cards
  - Cryptographic Testing
  - Cryptographic Analysis
- This research has advanced science and contributed to new or emerging standards, such as
  - Enhanced block ciphers (AES)
  - Faster and more secure hash algorithms (SHA-3)
  - Identity management (Personal Identity Verification)
- These standards have spawned new research avenues, so the cycle continues…

Success Criteria for Research

- NIST has succeeded if research
  - Moves the state of the art forward
  - Leads to more precise metrics or more cost-effective testing and validation; or
  - Most importantly, contributes to development of successful new standards

Success Criteria for Standards

- NIST has succeeded if products that conform to a standard are
  - Widely available & adopted
  - Interoperable
  - Satisfy customer requirements
    - Functionality
    - Performance
    - ROI