NIST and US Civilian Agency Cryptography

Matthew Scholl
Group Manager, Computer Security Division, ITL, NIST
Agenda:

- What is Crypto?
- What is Good Crypto?
- How you can Find the Good Stuff?
- When Good Crypto Goes Bad?
What is Crypto?

- Algorithms (the hard stuff)
- Key Management (the really hard stuff)
- Implementation (the hardest stuff)
The Algorithms

- Algorithms authorized for use by the US Civilian Agencies are specified in
  - FIPS 186-3 Secure Hash Standards
  - FIPS 197 Advanced Encryption Standard
  - FIPS 198-1 Keyed Hash Message Authentication Code
The Algorithms

- AES, TDEA, DSA, RSA, ECDSA and then,
- Modes of Operation: (Nine Total,)
- Modes provide algorithmic implementation for specific cryptographic needs;
  - Confidentiality (ECB, CBC, OFB, CFB, CTR, XTS-AES)
  - Authentication (CMAC)
  - Confidentiality and Authentication (CCM and GCM)
Key Management
(SP 800-57)

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

• Key Life spans (crypto periods)

• Public/Private Keys
  – Key Distribution
  – Key Validation
  – Key Revocation
Implementations

• Passwords/Pins/Entropy
• Authentication and Authorizations
• Communication Channels
• The other protections...
  – Physical/Environmental/Side Channel etc
What is Good Crypto?

- Does the product do what is claimed?
- Does it conform to standards?
- Was it independently tested?
- Is the product secure?
Good Crypto Metrics

- 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)
  - 26.5% Security Flaws
  - 65.1% FIPS Interpretation and Documentation Errors

- Areas of Greatest Difficulty
  - Physical Security
  - Self Tests
  - Random Number Generation
  - Key Management
Using 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
FIPS 140-2: Security Areas

1. Cryptographic Module Specification
2. Cryptographic Module Ports and Interfaces
3. Roles, Services, and Authentication
4. Finite State Model
5. Physical Security
6. Operational Environment
7. Cryptographic Key Management
8. EMI/EMC requirements
9. Self Tests
10. Design Assurance
11. Mitigation of Other Attacks
FIPS 140-2: Security Levels

- Level 1 is the lowest, Level 4 most stringent
- Requirements are primarily cumulative by level
- Overall rating is lowest rating in all sections
- Validation is applicable when a module is configured and operated in accordance with the level to which it was tested and validated
• Certificate number
• Vendor Name
  – Address
  – Contact
• Module Name
  – Version
  – Security Policy
  – Certificate
• Module Type
• Validation Date
• Overall Level
  – Section Levels
  – Algorithms
  – Embodiment
  – Vendor supplied text
• Certificate number
• Vendor Name
  – Address
  – Contact
• Module Name
  – Version
  – Security Policy
  – Certificate
  – Product Link
• Module Type
• Validation Date
• Overall Level
  – Section Levels and Operating Systems
  – Algorithms
  – Embodiment
  – Vendor supplied text
When Good Crypto Goes Bad

• Cryptography used to protect sensitive information
• Attackers are becoming smarter and computers are becoming more powerful
• Many commonly used crypto algorithms broken (e.g., DES broken about 1998, and SHA-1 weakened by attacks in 2005)
• Defensive measures? Use other algorithms and larger key sizes
The Good, The Bad, The Ugly

- Problem? How to transition?
- Solution: Be flexible and plan ahead
  - Strategy originally proposed in Draft SP 800-57, Part 1 in 2003
  - SP 800-57, Part 1 completed in 2005; revisions in 2006 and 2007
  - Goal: to transition from a security strength of 80 bits to 112 bits by 2011
    - Some algorithms no longer recommended
    - Larger key sizes required
Purpose of SP 800-131:

• To bring more specific transition details to the attention of the Federal government agencies and the public
• Written from the point of view of the CMVP: what new validations are allowed vs. what already-validated implementations will continue to be allowed
• Will be used to develop validation guidance documents
Encryption:

- Algorithms **no longer approved** after 2010:
  - Two-key Triple DES
  - SKIPJACK
- Algorithms (and key sizes) **approved** after 2010
  - Three-key Triple DES
  - AES 128, 192 and 256
Q: How do I know what Crypto algorithms and key sizes I’m using?

A: Check the technical specifications for your product and/or its cryptographic module. Also, the Cryptographic Algorithm Validation Program certificate will state what cryptographic algorithms are included in the module (see http://csrc.nist.gov/groups/STM/cmvp/validation.html).
Q: I am currently using FIPS 140-validated cryptography, isn’t that good enough?

A: Not quite; the product specifications and certificates should be checked. Transitions from specific algorithms and key sizes means that some certificates may need to be modified or invalidated. NIST plans to review previously-validated modules to remove the un-approved cryptography from our certificate listing, but this will take longer than the planned transition dates.
Q: Will the transition dates change?

A: NIST believes that the threats and vulnerabilities will only increase, and to push dates out further will continue to put our information at risk at an increasing level as time and technology progresses.
Issues re Impact and Implementation (4):

Q: How do I know where Cryptography is being used in my enterprise?

A: Agency CIOs, SAISOs, System Owners and Enterprise Architects should be able to identify where cryptography is being used in your enterprise, what types are being used and where. Also, these same people should be sure that these cryptographic transition requirements are planned for in systems under development or in procurement.
Issues re Impact and Implementation (5):

Q: Will I need to replace items, get them patched or updated, or can I evolve these items through my normal IT refresh cycle?

A: This is a policy decision that must be made by agency management officials and the Office of Management and Budget (OMB) by considering resources, risk and competing requirements. The ability to patch, update or use another cryptographic option that is approved in your current modules will depend on each product.
Issues re Impact and Implementation (6):

Q: Will this affect my ability to interoperate with other agencies or other organizations?

A: It might. Organizations who do not update their cryptography might have interoperability issues with organizations that do. Each interconnection should be evaluated for interoperability and transition schedules, or dual capabilities should be evaluated if needed to meet mission requirements.
Q: How can I still verify signatures in my archives or from organizations that are using old algorithms or key sizes (e.g., 1024-bit RSA and DSA, and 160-bit ECDSA)?

A: The verification capability for these algorithms and key sizes will continue to be approved. The public keys for these signatures need to be saved (e.g., archived); The signing keys need to be destroyed to preclude further use.
Issues re Impact and Implementation (8):

Q: Are modules containing algorithms and key sizes approved after 2010 currently available commercially?

A: Yes, modules with algorithms and key sizes that provide a security strength of 112 bits or higher have been available for some time. However, some protocols may or may not use or provide some of these capabilities yet. Consult your current vendors and contractors.
Issues re Impact and Implementation (9):

Q: Will I still need to be sure any upgrades that are installed are still FIPS 140-2 compliant?

A: Yes, it is important that agencies use cryptographic modules that have been validated for correctness. If the data is important enough to use cryptography, then it’s important enough to ensure that it is correct.
QUESTIONS ?
BACKGROUND
Digital Signatures:

• Transition from 186-2 to 186-3 by 2011
• FIPS 186-2 certificates will continue to be valid, subject to the requirements for appropriate security strengths:
  – Signature generation: ≥ 112 bits of security (e.g., ≥ 2048-bit keys for DSA and RSA; ≥ 224-bit keys for ECDSA)
  – Signature verification: ≥ 80 bits of security when generated
• The invalidation of the algorithm certificates will affect all currently-validated FIPS 186-2 DSA implementations, as well as those implementations of RSA and ECDSA that only use SHA-1 for digital signature generation
Random Number Generation:

  - No new validations after 2010
  - Already-validated implementations OK thru 2015
- RNGs specified in SP 800-90
  - Approved beyond 2010
  - Part of a larger effort within ANSI
  - Provides more guidance, including requirements for achieving higher security strengths
Key Wrapping:

• Encryption of one key by another, possibly including an integrity mechanism
• No FIPS or NIST Recommendation yet.
• IG D.2: AES or Triple DES may be used to wrap keys using the specification on the NIST web site.
  – Two-key Triple DES OK thru 2010
  – AES and Three-key Triple DES OK beyond 2010
Deriving Keys from a Key (a.k.a. Key Derivation):

- Specified in SP 800-108
- HMAC–based KDF using any approved hash function OK (HMAC specified in FIPS 198-1)
- CMAC-based KDF (CMAC specified in SP 800-38B):
  - Two-key Triple DES OK thru 2010
  - AES and Three-key Triple DES OK beyond 2010
Hash Functions (FIPS 180-3):

• SHA-1:
  – OK for digital signature generation thru 2010
  – OK for digital signature verification beyond 2010
  – OK for other applications beyond 2010 (e.g., HMAC, RNGs, KDFs)

• SHA-224, SHA-256, SHA-384, SHA-512:
  – OK for all applications (including digital signature generation and verification) beyond 2010
Message Authentication Codes:

- HMAC (FIPS 198-1 and SP 800-107):
  - Any approved hash function
  - Key lengths $\geq 80$ bits OK thru 2010
  - Key lengths $\geq 112$ bits OK beyond 2010
- CMAC (SP 800-38B):
  - Two-key Triple DES OK thru 2010
  - AES and Three-key Triple DES OK beyond 2010