Suite B Cryptography

March 22, 2006

Elaine Barker

ebarker@nist.gov

301-975-2911

Background

- NIST algorithms not used for classified data
- NIST & NSA coordinating standardized public algorithms
- NSA selected a subset of NIST algorithms for classified applications through TOP SECRET: see http://www.nsa.gov/ia/
- NSA approval still required for implementations and systems that are used to protect classified information

CNSSP #15

- Committee on National Security Systems Policy No. 15
- 128-bit AES can be used for up thru SECRET
- 192 & 256 bit AES can be used for up thru TOP SECRET
- http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf

Suite B

- FIPS 140 Cryptographic Module Validation required for unclassified applications
- NSA will evaluate products used for classified applications
  - Commercial COMSEC Evaluation Program (CCEP) and User Partnership Agreements (UPA)
    - Use Suite B algorithms
    - Provide extensive design guidance

Suite B – the algorithms

- Encryption Algorithm AES (FIPS 197)
  - AES-128 up thru SECRET
  - AES-256 up thru TOP SECRET
- Digital Signature (Draft FIPS 186-3)
  - ECDSA with 256-bit prime modulus up thru SECRET
  - ECDSA with 384-bit prime modulus up thru TOP SECRET

Suite B – the algorithms (contd.)

- Key Agreement (NIST SP 800-56A)
  - EC Diffie-Hellman or EC MQV with 256-bit prime modulus up thru SECRET
  - EC Diffie-Hellman or EC MQV with 384-bit prime modulus up thru TOP SECRET
- Hash Functions (FIPS 180-2)
  - SHA-256 up thru SECRET
  - SHA-384 up thru TOP SECRET

Comparable Security Strengths

Security Strength	Symmetric Key Algorithms	FFC (DSA, D-H, MQV)	IFC (RSA)	ECC (ECDSA, ECDH, ECMQV)
80	2TDEA[1]	1024	1024	160-223
112	3TDEA	2048	2048	224-255
128	AES-128	3072	3072	256-383
192	AES-192	7680	7680	384-511
256	AES-256	15360	15360	512+

[1] The guarantee of at least 80-bits of security for 2TDEA is based on the assumption that an attacker has at most 2^{40} matched plaintext and ciphertext blocks.

FFC = Finite Field Cryptography
IFC = Integer Factorization Cryptography
ECC = Elliptic Curve Cryptography

Comparable Security Strengths (contd.)

Security Strength	Digital Signatures and Hash-Only Applications	HMAC, Key Derivation Functions & Random Number Generation[1]
80	SHA-1[2]	
112	SHA-224	
128	SHA-256	SHA-1
192	SHA-384	SHA-224
256	SHA-512	SHA-256
> 256		SHA-384, SHA-512

[1] The security strength assumes that the random number generator has been provided with adequate entropy to support the desired security strength.

[2] A recent attack on SHA-1 claims that SHA-1 provides less than 80 bits of security for digital signatures; the claimed security strength for digital signatures is 63 - 69 bits.

Encryption Algorithms

	Unclassified Use		**Suite B**	
	Min. 80-bit Strength Through 2010	**Min. 112-bit Strength After 2010**	**SECRET**	**TOP SECRET**
AES				
128	√	√	√	
192	√	√		
256	√	√	√	√
TDES				
2key TDES	√			
3key TDES	√	√		

Hash Functions (for Digital Signatures)

	Unclassified use		Suite B	
	Min. 80-bit Strength Through 2010	**Min. 112-bit Strength After 2010**	**SECRET**	**TOP SECRET**
SHA-1	√			
SHA-224	√	√		
SHA-256	√	√	√	
SHA-384	√	√	√	√
SHA-512	√	√		

Digital Signatures

	Unclassified use		Suite B	
	Min. 80-bit Strength Through 2010	Min. 112-bit Strength After 2010	SECRET	TOP SECRET
DSA & RSA				
1024	√			
2048	√	√		
3072	√	√		
ECDSA				
160	√			
224	√	√		
256	√	√	√*	
384	√	√	√*	√*
512	√	√		

* Prime Modulus curves only

Key Agreement

	Unclassified Use		Suite B	
	Min. 80-bit Strength Through 2010	Min. 112-bit Strength After 2010	SECRET	TOP SECRET
Diffie-Hellman, MQV or RSA				
1024	√			
2048	√	√		
EC Diffie-Hellman or EC MQV				
160	√			
224	√	√		
256	√	√	√*	
384	√	√	√*	√*
512	√	√		

* Prime Modulus curves only

Why AES-256 and ECC-384 in Suite B?

- Theoretically:
  - AES-256 is equivalent to ECC-512
  - AES-192 is equivalent to ECC-384
- CNSSP # 15: AES-192 for TOP SECRET
  - AES-192 not included in Suite B
- AES-256 with ECC-384 seems a mismatch
  - Little performance penalty for AES-256 over AES-192
  - Many implementers choosing to use AES-256
  - Significant performance cost for ECC-512 compared to ECC-384
  - ECC-384 is strong enough for TOP SECRET
  - Make life simple: use ECC-384, which is fast and strong enough, with AES-256 which is strong and fast enough.

Suite B: Bottom Line

- Some users need have both classified and unclassified applications
- National security applications need to use COTS products
- No fundamental difference between algorithms for SBU & classified data
- NIST & NSA cooperation: cryptography for both SBU and classified data
- NSA approval of implementations required for classified data
  - Expect NSA-managed keying material for classified applications
- Unclassified users must have CMVP-validated crypto modules
  - More choices of algorithms than in Suite B
  - Users typically generate their own keys

NIST Links

- NIST Computer Security Resources Center
  - http://csrc.nist.gov/
- NIST Crypto toolkit
  - http://csrc.nist.gov/CryptoToolkit/
- FIPS page
  - http://csrc.nist.gov/publications/fips/index.html
- NIST Security Special Publications
  - http://csrc.nist.gov/publications/fips/index.html

Questions ?