National Security Agency Perspective on Key Management

IEEE Key Management Summit
5 May 2010

Petrina Gillman
Information Assurance (IA)
Infrastructure Development & Operations
Technical Director
National Security Agency
(301) 688-8133
plgillm@nsa.gov

Agenda

- NSA Information Assurance (IA) Mission
- Secure Information Sharing Needs
- NSA Initiatives

NSA IA Mission

- Focused on Protecting US National Security Information and Information Systems
- National Security Systems are defined in Title 44 U.S. Code Section 3542, Federal Information Security Management Act of 2003. Includes systems that:
  - Involve intelligence activities
  - Cryptologic activities related to national security
  - Equipment that is an integral part of a weapon or weapons system
  - Critical to the direct fulfillment of military or intellitgence mission
  - Classified information

Secure Information Sharing

- Secure Information Sharing requirements motivates the need for widespread cryptographic interoperability.
- Operational cryptographic interoperability needs include:
  - Enable the US Government to securely share intelligence information with state and local First Responders
  - Enable War fighters to securely share information on the battlefield with non-traditional coalition partners.

NSA Initiatives

- Commercial Solutions Partnership Program
- Cryptographic Interoperability Strategy (CIS)

Commercial Solutions Partnership Program

- Enable the use of a combination of COTS Information Assurance products composed to form a solution to protect information up to the Secret level
- Products used in CSPP solutions must be successfully evaluated under National Information Assurance Partnership Program and the NIST Cryptographic Module Validation Program
  - National Information Assurance Partnership (NIAP) process will utilize new Standard Protection Profiles. More info at: http://www.niap-ccevs.org
  - NIST Cryptographic Module Validation Program for FIPS 140-3 requirements
- Cryptographic Interoperability Strategy (CIS) / Suite B

CIS/Suite B Cryptographic Algorithms

Algorithm	Bit Size	Function	Standard
ECDSA	256 / 384	Signature	FIPS 186-3
AES	128 / 256	Symmetric Encryption	FIPS 197
ECDH	256 / 384	Key Exchange	SP 800-56A
SHA	256 / 384	Hashing	FIPS 180-3

- Lower key sizes are acceptable for protecting up to SECRET information.
- Protecting Top Secret information requires the use of 256 bit AES keys, 384-bit prime modulus elliptic curve and SHA 384 as well as other controls on manufacture, handling and keying.

http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

Suite B Cryptography for Internet Protocols

- IPsec: IETF RFC 4869 "Suite B Cryptography for IPsec"
- TLS: IETF RFC 5430 "Suite B Cipher Suites for TLS; "TLS Elliptic Curver Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)
- S/MIME: "Suite B in Secure/Multipurpose Internet Mail Extensions (S/MIME)
- SSH: IETF RFC 5647 "AES Galois Counter Mode for the Secure Shell Transport Layer Protocol"

Suite B Implementation Guides

- Suite B Implementer's Guide to FIPS 186-3
  - Specifies the Elliptic Curve Digital Signature Algorithm from FIPS 186-3, Digital Signature Standard, to be used in future and existing cryptographic protocols for Suite B products
- Includes the Suite B elliptic curve domain parameters
- Provides example data for the ECDSA signature algorithm and auxiliary functions necessary for ECDSA implementations to comply with FIPS 186-3 and Suite B

Suite B Implementation Guides (cont.)

- Suite B Implementer's Guide to NIST SP 800-56A
  - Details the specific Elliptic Curve Diffie Hellman (ECDH) key-agreement schemes from NIST SP 800-56A: Recommendation for Pair-Wise Key Establishment Schemes using Discrete Logarithm Cryptography to be used in future and existing cryptographic protocols for Suite B products
  - http://www.nsa.gov/ia/_files/SuiteB_Implementer_G-113808.pdf
- Includes the Suite B elliptic curves and domain parameters, key generation methods & key derivation functions
- Companion Document: Mathematical Routines for NIST Prime Elliptic Curves. http://www.nsa.gov/ia/_files/nist-routines.pdf

Public Key Certificates & Certificate Processing

- Base Suite B Certificate and CRL profile
  - -IETF RFC 5759 Suite B Certificate and Certificate Revocation List Profile
  - -Profile of IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile
- Implementations need to meet both Certificate and CRL formats and certificate and CRL processing requirements
- Some US national security communities have additional requirements that build upon the base profile. NSA can provide this additional guidance upon request.

Trust Anchors & Trust Anchor Management

- Trust Anchors
  - Draft-ietf-pkix-ta-format-04
- Trust Anchor Management
  - Draft-ietf-pkix-tamp-07
- Both standards are in the IETF RFC editors queue. Should be assigned RFC numbers shortly.

Certificate Management

- Supports requesting certificate signing services & receiving response
- Suite B Profile of Certificate Management over Cryptographic Message Syntax (CMS)
  - Draft-turner-SuiteB-CMC-00.txt
  - Profile and refinement of:
    - RFC 5272 Certificate Management Over CMS, June 2008
    - RFC 5273 Certificate Management Over CMS (CMC): Transport Protocols, June 2008
    - RFC 5274 Certificate Management Messages over CMS (CMC): Compliance Requirements, June 2008

Suite B Key Delivery Protocol

- Protocol to provision devices with cryptographic keys and other security objects from a provisioning infrastructure
- Cryptographic keys and other security objects are cryptographically protected all the way from the provisioning infrastructure into the devices
- Devices can retrieve cryptographic keys and other security objects directly from the infrastructure or via an intermediary
  - Keys are encrypted, by the infrastructure, for specific devices
  - Device unwraps key package within security boundary

Suite B Key Delivery Protocol Algorithms

Key Packaging Algorithm Suite	
Security Service	**Algorithm(s)**
Message Digest	SHA-384
Signature	ECDSA-384
Content Encryption	AES key Wrap (256) with Message Length Indicator
Key Encryption	AES key Wrap (256) with Message Length Indicator
Key Agreement	Ephemeral-Static ECDH-384
Message Authentication Code	HMAC-SHA-384

Suite B Key Delivery Protocol Design

- Protocol utilizes and profiles commercial standards including:
  - RFC 5652 Cryptographic Message Syntax\
    - Sign, encrypt and authenticate message content
  - Draft-ietf-pkix-ta-format-04 & Draft-ietf-pkix-tamp-07
  - RFC 5430 Suite B Profile for Transport Layer Security
  - HTTP protocols (RFC 2616, 2617, 2618)
- Soliciting Industry comments
  - Please contact me for a copy of the specification

Contact Information

Petrina Gillman
(301) 688-8133
plgillm@nsa.gov

Commercial Solutions Partnership Program
NSA Commercial Solutions Center
(240)373-4163
Attn: Industry Support Team
9800 Savage Road Suite 6944
Ft. Meade MD. 20755-6844

Questions