Kerberos and Suite B

Kelley Burgin

National Security Agency

October 30, 2012

What is Suite B?

Cryptographic Interoperability Strategy (CIS)

- Interoperability at the speed of business
- Commercial Solutions for Classified (CSfC)
  - Speedy solution (GOTS = 4/5 years)
  - Use COTS in a "layered" solution to protect classified info
  - NIAP Protection Profiles
- Suite B
  - Set of NIST-approved public algorithms
  - Suite B profile for public protocols to use in each "layer"

Where is Suite B?

Suite B profiles exist in RFCs for:

- IPsec
  - RFC 6379 Suite B Cryptographic Suites for IPsec
  - RFC 6380 Suite B Profile for IPsec
- TLS
  - RFC 6460 Suite B Profile for TLS
- S/MIME
  - RFC 6318 Suite B in S/MIME
- SSH
  - RFC 5647 AES GCM for the SSH Transport Layer Protocol
  - RFC 6239 Suite B Cryptographic Suites for SSH

Suite B Algorithms

	minLOS 128	minLOS 192
Encryption	AES 128	AES 256
Hashing	SHA-256	SHA-384
Key Exchange	ECDH p256	ECDH p384
Signing	ECDSA with p256 SHA-256	ECDSA with p384 SHA-384

Notes

- No mode specified
- No SHA-1 anywhere
- CRL checking required

What this means for Kerberos

- PKINIT required
  - No password-based keys
  - ECDSA for authentication
  - Ephemeral-ephemeral ECDH for key exchange
- Encryption with AES in CBC mode (CTS)
  - Aligned with McGrew's AEAD draft
- Message integrity is provided by SHA-2 HMAC
- Use algorithm-agility draft
  - Remove hardcoded SHA-1 checksum over AS REQ
  - Add KDF that uses SHA-2

References

- draft-burgin-kerberos-aes-cbc-hmac-sha2
- draft-burgin-kerberos-suiteb
- draft-mcgrew-aead-aes-cbc-hmac-sha2
- draft-ietf-krb-wg-pkinit-alg-agility

Are we done??

Questions?