What is Suite B?

How does it relate to Government Certifications?

Acumen Security

Agenda – What are we going to do?

- Who am I?
- A little background on Suite-B.
- Suite-B: What's covered.
- How does Suite-B relate to your favorite cryptographic protocol?
- What about the certifications you get for your products?

Introduction

- 13 years of industry experience
- Unique perspective:
  - Part of a couple certification labs
  - Part of a product vendor
- Started Acumen Security in 2014

Background

Acumen Security

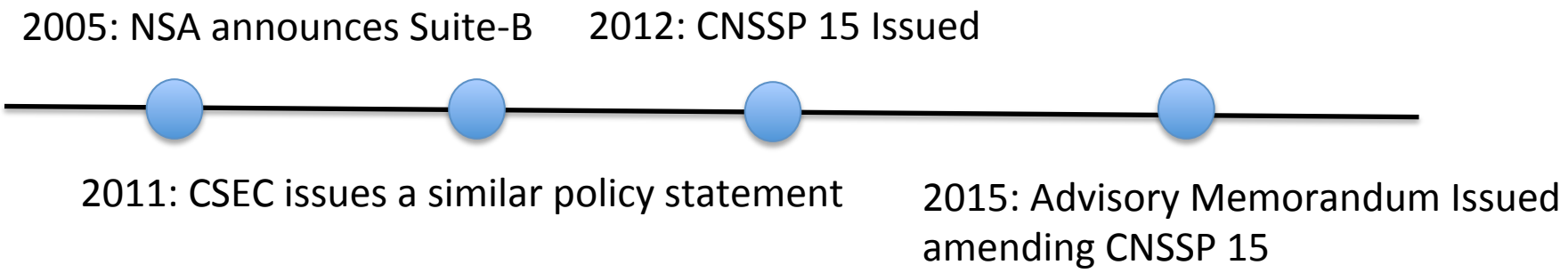
What is Suite-B & Why do we care?

- U.S government faced a problem, the cost of developing purpose-built GOTS cryptography was neither cost efficient nor effective.
- Industry could deliver solutions that met the gov't requirements for all but a small fraction of its use cases
- Price point/timeframe significantly less than in-house solutions.
- NSA adopted a suite of commercially available cryptographic algorithms that could be used to protect data through TOP SECRET classification

This is Suite-B!

- Suite-B represents the strongest, most secure, and most efficient commercial cryptography available.

History of Suite-B: A timeline



Minimum Level of Security (minLOS)

- Defines classification of data that may be protected by a certain algorithm
- Historical concept
- All algorithms now defined for protecting up to TOP SECRET previous minLOS of protecting up to SECRET has been removed
- Previous minLOS Classifications:
  - minLOS of 128-bits of security for protecting up to SECRET (historical)
  - minLOS of 192-bits of security for protecting up to TOP SECRET

What is covered?

- Symmetric cipher used for information protection (bulk encryption/ decryption)
- Asymmetric algorithms used for key establishment
- Asymmetric algorithms used for digital signatures
- Algorithms used for computing a condensed representation of information (hashing)

Allowed Algorithms

Historical vs. Current

	Historical	Current
Bulk Encryption	minLOS 128: AES-128 minLOS 192: AES-256	AES-256
Key Establishment	minLOS 128: ECDH 256-bit random ECP group minLOS 192: ECDH 384-bit random ECP group	ECDH 384-bit random ECP group FFCDH 3072-bit modulus RSA 3072-bit modulus
Digital Signatures	minLOS 128: ECDSA-256 minLOS 192: ECDSA-384	ECDSA-384 RSA 3072-bit modulus
Hashing	minLOS 128: SHA-256 minLOS 192: SHA-384	SHA-384

Protocols

Acumen Security

Suite-B and Protocols

- RFCs created for common protocols
  - RFC 6239 - Suite B SSH algorithms
  - RFC 5656 - EC as used in SSH
  - RFC 6187 - X.509v3 Certificates for SSH Auth
  - RFC 6460 - Suite B Profile for TLS
  - RFC 6379 - Suite B Cryptographic Suites for IPsec
  - RFC 6380 - Suite B Profile for Internet Protocol Security (IPsec)
- Disclaimers:
  - These were all written before new guidance
  - NSA is considering how to handle previously written RFCs

Suite-B in SSH

- **Note**: This presents what is in the RFC. The portions that continue to meet NSA guidance are presented in **BOLD GREEN**

minLOS	Encryption/Integrity	Key Exchange		Authentication		
		ECDH Group	Hash	Certificate Format	Signature Algorithm	Hash
128-bit	AES-GCM (128-bit)	ECDH 256-bit random ECP group	SHA-256	X.509 v3	ECDSA on P-256	SHA-256
RFC ID	AEAD_AES_128_GCM	ecdh-sha2-nistp256		x509v3-ecdsa-sha2-nistp256		
192-bit	**AES-GCM (256-bit)**	**ECDH 384-bit random ECP group**	**SHA-384**	**X.509 v3**	**ECDSA on P-384**	**SHA-384**
RFC ID	**AEAD_AES_256_GCM**	**ecdh-sha2-nistp384**		**x509v3-ecdsa-sha2-nistp384**		

Suite-B in IKE/IPsec

- **Note**: This presents what is in the RFC. The portions that continue to meet NSA guidance are presented in **BOLD GREEN**

minLOS	Option	Use Case	Encryption	Integrity	PRF	KEX	Authentication	IANA ID
128-bit	ESP	Integrity & Encryption	AES-GCM (128-bit) with 16-octet ICV	NULL	N/A	N/A	N/A	Suite-B-GCM-128
		Integrity Only	NULL	AES-GMAC (128-bit)	N/A	N/A	N/A	Suite-B-GMAC-128
	IKEv2	All	AES-CBC (128-bit)	HMAC-SHA-256-128	HMAC-SHA-256	ECDH 256-bit random ECP group	ECDSA-256 or ECDSA-384	Included in both: Suite-B-GCM-128/ Suite-B-GMAC-128
192-bit	**ESP**	**Integrity & Encryption**	**AES-GCM (256-bit) with 16-octet ICV**	**NULL**	**N/A**	**N/A**	**N/A**	**Suite-B-GCM-256**
		Integrity Only	**NULL**	**AES-GMAC (256-bit)**	**N/A**	**N/A**	**N/A**	**Suite-B-GMAC-256**
	IKEv2	**All**	**AES-CBC (256-bit)**	**HMAC-SHA-384-192**	**HMAC-SHA-384**	**ECDH 384-bit random ECP group**	**ECDSA-384 (only)**	**Included in both: Suite-B-GCM-256/ Suite-B-GMAC-256**
NOTE: AH is not permitted for Suite-B IKE/IPsec connections								

Suite-B in TLS

- **Note**: This presents what is in the RFC. The portions that continue to meet NSA guidance are presented in **BOLD GREEN**

minLOS	Encryption/ Integrity	PRF	KEX	Authentication	Cipher Suite ID(s)	Protocol Version
128-bit	AES-GCM (128-bit)	TLS PRF with SHA-256	ECDH 256-bit random ECP group	ECDSA-256 or ECDSA-384	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, or, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	**TLS 1.2 (only)**
192-bit	**AES-GCM (256-bit)**	**TLS PRF with SHA-384**	**ECDH 384-bit random ECP group**	**ECDSA-384 (only)**	**TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (only)**	

Suite-B and Certifications

Acumen Security

Suite-B and FIPS 140

- The algorithmic components included in Suite-B are all CAVP testable
- As part of the FIPS certification, each algorithm should be tested
- Per protocol-basis:
  - IKE/IPsec:
    - All algorithms should be tested
    - KDF should be tested
    - ESP Mode approved mode
  - TLS
    - All algorithms should be tested
    - KDF should be tested
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 approved ciphersuite
    - TLS 1.2 approved protocol version
  - ***SSH***
    - ***CANNOT be FIPS'd***
    - ***AES-GCM is non-approved for SSH***

Suite-B and Common Criteria (1/2)

- NDcPP will be used as an example
- SFRs:
  - FCS_CKM.1: RSA, DSA, ECDSA included in SFR
    - Must use 3072-bit keys, curve P-384
  - FCS_CKM.2: FFCDH, ECDH, RSA included in SFR
    - Must use 3072-bit keys/modulus, NSA specified curves
  - FCS_COP.1(1): AES-GCM included in SFR
    - Must use 256-bits keys
  - FCS_COP.1(2): RSA, ECDSA included in SFR
    - Must use 3072-bit keys, curve P-384
  - FCS_COP.1(3): SHA-384 included in SFR

Suite-B and Common Criteria (2/2)

- SFRs:
  - FCS_TLSC_EXT.1/ FCS_TLSS_EXT.1 :
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 included in SFR
    - TLS 1.2 required by SFR
    - NOTE: This SFR does not mandate that the TLS ciphersuite be advertised first
  - FCS_SSHC_EXT.1/ FCS_SSHS_EXT.1
    - x509v3-ecdsa-sha2-nistp384 is allowed by the SFR
    - The integrity, bulk encryption/decryption/hashing is drawn from FCS_COP.1(*) SFRs which include all Suite-B algorithms
  - FCS_IPSEC_EXT.1:
    - AES-GCM is selectable in SFR
    - ESP is required by SFR
    - ECDH Group 20 (384-bit Random ECP) is selectable

Suite-B and CSFC

- Specifies SFR selections required in CC evaluations.
- TLS Protected Server:
  - FCS_TLSC_EXT.1/ FCS_TLSS_EXT.1 (note these are actually referred to as FCS_TLS.1 in the component definition):
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (Suite-B approved) is a required selection
- VPN Gateway:
  - FCS_COP.1(1):
    - AES-GCM is a required selection
  - FCS_COP.1(2):
    - ECDSA with P-384 is a required selection
  - FCS_COP.1(3):
    - SHA-384 is a required selection
  - FCS_IPSEC_EXT.1:
    - AES-GCM is a required selection
    - ECDH Group 20 is a required selection

Suite-B and Certifications Wrap Up

- CC Protection Profiles can (and have) been crafted in a way to allow Suite-B cryptography
- FIPS 140 products can be built using the Suite-B algorithms in a compliant manner
- Except for SSH which cannot use AES-GCM in a FIPS-approved mode of operation
- The CC selections required by CSFC are unsurprisingly consistent with Suite-B cryptography
- In short,

Suite-B and certifications play nice together!

(for the most part)

What's next??

Acumen Security

Things to Come

- NSA has posted that another revision is coming
- Quantum resistant cryptography
- Revision to CNSSP-15
- Others?

Conclusion

- Gave background on Suite-B
- Identified “Suite-B Crypto”
- Described how Suite-B can be used in common protocols
- Discussed how Suite-B plays with certification

Thank you!

Acumen Security