Internet Engineering Task Force (IETF)
Request for Comments: 6380
Category: Informational
ISSN: 2070-1721

K. Burgin
National Security Agency
M. Peck
The MITRE Corporation

October 2011

Suite B Profile for Internet Protocol Security (IPsec)

Abstract

The United States Government has published guidelines for "NSA Suite B Cryptography" dated July, 2005, which defines cryptographic algorithm policy for national security applications. This document specifies the conventions for using Suite B cryptography in IP Security (IPsec).

Since many of the Suite B algorithms are used in other environments, the majority of the conventions needed for the Suite B algorithms are already specified in other documents. This document references the source of these conventions, with some relevant detail repeated to aid developers who choose to support Suite B.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6380.

Table of Contents

1. Introduction

This document specifies the conventions for using NSA Suite B Cryptography [SuiteB] in IP Security (IPsec).

IP Security (IPsec) provides confidentiality, data integrity, access control, and data source authentication to IP datagrams. The Internet Key Exchange (IKE) provides an automated key management for IPsec, performing mutual authentication between two parties and establishing security associations (SAs) that protects both IKE and IPsec communications. Suite B compliant implementations for IPsec MUST use IKEv2 [RFC5996].

[RFC6379] defines a set of four cryptographic user interface suites for IPsec that are comprised of Suite B algorithms. The four suites specify options for IKEv2 and for the IP Encapsulating Security Payload (ESP), [RFC4303]. Suite B compliant implementations for IPsec MUST use one of these four suites depending upon the desired security level and security services.

2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Suite B Requirements

Suite B requires that key establishment and signature algorithms be based upon Elliptic Curve Cryptography and that the encryption algorithm be AES [FIPS197]. Suite B includes [SuiteB]:

Encryption:	Advanced Encryption Standard (AES) (key sizes of 128 and 256 bits)
Digital Signature	Elliptic Curve Digital Signature Algorithm (ECDSA) [FIPS186-3] (using the curves with 256- and 384-bit prime moduli)
Key Exchange	Elliptic Curve Diffie-Hellman (ECDH) [SP800-56A], (using the curves with 256- and 384-bit prime moduli)
Hashes	SHA-256 and SHA-384 [FIPS180-3]

The two elliptic curves used in Suite B appear in the literature under two different names. For the sake of clarity, we list both names below:

Curve	NIST name	SECG name	IANA assigned DH group #
P-256	nistp256	secp256r1	19
P-384	nistp384	secp384r1	20

IANA has already registered these DH groups in [IKEV2IANA].

4. Minimum Levels of Security (minLOS)

Suite B provides for two levels of cryptographic security, namely a 128-bit minimum level of security (minLOS_128) and a 192-bit minimum level of security (minLOS_192). Each level defines a minimum strength that all cryptographic algorithms must provide.

4.1. Non-Signature Primitives

We divide the Suite B non-signature primitives into two columns as shown in Table 1.

	Column 1	Column 2
Encryption	AES-128	AES-256
Key Agreement	ECDH on P-256	ECDH on P-384
Hash for PRF/MAC	SHA256	SHA384

Table 1: Suite B Cryptographic Non-Signature Primitives

At the 128-bit minimum level of security:

- the non-signature primitives MUST either come exclusively from Column 1 or exclusively from Column 2.

At the 192-bit minimum level of security:

- the non-signature primitives MUST come exclusively from Column 2.

4.2. Suite B IPsec Cryptographic Suites

Each system MUST specify a security level of a minimum of 128 bits or 192 bits. The security level determines which suites from [RFC6379] are allowed.

The four Suite B cryptographic user interface suites ("UI suites") [RFC6379]: Suite-B-GCM-128, Suite-B-GMAC-128, Suite-B-GCM-256 or Suite-B-GMAC-256, satisfy the requirements of Section 3.

At the 128-bit minimum level of security:

- one of Suite-B-GCM-128, Suite-B-GMAC-128, Suite-B-GCM-256 or Suite-B-GMAC-256 MUST be used by Suite B IPsec compliant implementations [RFC6379].

At the 192-bit minimum level of security:

- one of Suite-B-GCM-256 or Suite-B-GMAC-256 MUST be used by Suite B IPsec compliant implementations [RFC6379].

4.3. Suite B IKEv2 Authentication

Digital signatures using ECDSA MUST be used for authentication by Suite B compliant implementations. [RFC4754] defines two digital signature algorithms: ECDSA-256 and ECDSA-384. Following the direction of RFC 4754, ECDSA-256 represents an instantiation of the ECDSA algorithm using the P-256 curve and the SHA-256 hash function. ECDSA-384 represents an instantiation of the ECDSA algorithm using the P-384 curve and the SHA-384 hash function.

If configured at a minimum level of security of 128 bits, a system MUST use either ECDSA-256 or ECDSA-384 for IKE authentication. It is allowable for one party to authenticate with ECDSA-256 and the other party to authenticate with ECDSA-384. This flexibility will allow interoperability between an initiator and a responder that have different sizes of ECDSA authentication keys.

Initiators and responders in a system configured at a minimum level of security of 128 bits MUST be able to verify ECDSA-256 signatures and SHOULD be able to verify ECDSA-384 signatures.

If configured at a minimum level of security of 192 bits, ECDSA-384 MUST be used by both parties for IKEv2 authentication.

Initiators and responders in a system configured at a minimum level of security of 192 bits MUST be able to verify ECDSA-384 signatures.

For Suite B compliant systems, authentication methods other than ECDSA-256 and ECDSA-384 MUST NOT be used for IKEv2 authentication. If a relying party receives a message signed with any other authentication method, it MUST return an AUTHENTICATION_FAILED notification and stop processing the message.

4.4. Digital Signatures and Certificates

The initiator and responder, at both minimum levels of security, MUST each use an X.509 certificate that complies with the "Suite B Certificate and Certificate Revocation List (CRL) Profile" [RFC5759] and that contains an elliptic curve public key with the key usage bit set for digital signature.

5. Suite B Security Associations (SAs) for IKEv2 and IPsec

The four suites in [RFC6379] specify options for ESP [RFC4303] and IKEv2 [RFC5996]. The four suites are differentiated by cryptographic algorithm strength and a choice of whether ESP is to provide both confidentiality and integrity or integrity only. The suite names are based upon the AES mode ("GCM" or "GMAC") and the AES key length specified for ESP ("128" or "256"). Suites with "GCM" in their name MUST be used when ESP integrity protection and encryption are both needed. Suites with "GMAC" in their name MUST be used only when there is no need for ESP encryption.

An initiator in a system configured at a minimum level of security of 128 bits MUST offer one or more of the four suites: Suite-B-GCM-128, Suite-B-GMAC-128, Suite-B-GCM-256, or Suite-B-GMAC-256 [RFC6379]. Suite-B-GCM-128 and Suite-B-GMAC-128, if offered, MUST appear in the IKEv2 and IPsec SA payloads before any offerings of Suite-B-GCM-256 and Suite-B-GMAC-256.

A responder in a system configured at a minimum level of security of 128 bits MUST support one or both of the two suites Suite-B-GCM-128 or Suite-B-GMAC-128 and SHOULD support one or both of the two suites Suite-B-GCM-256 or Suite-B-GMAC-256. The responder MUST accept one of the Suite B UI suites. If none of the four suites are offered, the responder MUST return a Notify payload with the error "NO_PROPOSAL_CHOSEN" when operating in Suite B compliant mode.

An initiator in a system configured at a minimum level of security of 192 bits MUST offer either one or both suites: Suite-B-GCM-256 or Suite-B-GMAC-256.

A responder configured in a system at a minimum level of security of 192 bits MUST choose one of Suite-B-GCM-256 or Suite-B-GMAC-256. If neither suite is offered, the responder MUST return a Notify payload with the error "NO_PROPOSAL_CHOSEN".

6. The Key Exchange Payload in the IKE_SA_INIT Exchange

A Suite B IPsec compliant initiator and responder MUST each generate an ephemeral elliptic curve key pair to be used in the elliptic curve Diffie-Hellman (ECDH) key exchange. If the 256-bit random ECP group for Transform Type 4 is selected, each side MUST generate an EC key pair using the P-256 elliptic curve [SP800-57]. If the 384-bit random ECP group for Transform Type 4 is selected, each side MUST generate an EC key pair using the P-384 elliptic curve [SP800-57]. The ephemeral public keys MUST be stored in the key exchange payload as in [RFC5903].

7. Generating Keying Material for the IKE SA

The ECDH shared secret established during the key exchange consists of the x value of the ECDH common value [RFC5903]. The x value is 256 or 384 bits when using the P-256 or P-384 curve, respectively.

IKEv2 [RFC5996] allows for the reuse of Diffie-Hellman ephemeral keys. Section 5.6.4.3 of NIST SP800-56A states that an ephemeral private key MUST be used in exactly one key establishment transaction and MUST be zeroized after its use. Section 5.8 of SP800-56A states that the Diffie-Hellman shared secret MUST be zeroized immediately after its use. Suite B compliant IPsec systems MUST follow the mandates in SP800-56A.

If using PRF-HMAC-SHA-256, SKEYSEED, SK_d, SK_pi, and SK_pr MUST each be generated to be 256 bits long per RFC 5996 ([RFC5996], Section 2.14). If using PRF-HMAC-SHA-384, SKEYSEED, SK_d, SK_pi and SK_pr MUST each be generated to be 384 bits long. SK_ai and SK_ar MUST be 256 or 384 bits long if using HMAC-SHA-256-128 or HMAC-SHA-384-192, respectively. SK_ei and SK_er MUST be 128 or 256 bits long if the key length attribute for AES_ENC_CBC is set to 128 or 256, respectively.

8. Additional Requirements

AH is not supported in Suite B compliant implementations.

Per [RFC5996], although ESP does not directly include a Diffie-Hellman exchange, a Diffie-Hellman group MAY be negotiated for the Child SA. This allows the peers to employ Diffie-Hellman in the CREATE_CHILD_SA exchange. If a transform Type 4 is specified for an SA for ESP, the value of the transform MUST match that of the transform used by the IKE SA.

Per RFC 5996, if a CREATE_CHILD_SA exchange includes a KEi payload, at least one of the SA offers MUST include the Diffie-Hellman group of the KEi. For Suite B IPsec compliant implementations, the Diffie-Hellman group of the KEi MUST use the same random ECP group used in the IKE_INIT_SA.

For IKEv2, rekeying of the CREATE_CHILD_SA MUST be supported by both parties. The initiator of this exchange MAY include a new Diffie-Hellman key; if it is included, it MUST use the same random ECP group used in the IKE_INIT_SA. If the initiator of the exchange includes a Diffie-Hellman key, the responder MUST include a Diffie-Hellman key, and it MUST use the same random ECP group.

Suite B IPsec compliant systems MUST support IKEv2 and MUST NOT use IKEv1 between a Suite B compliant initiator and responder. To accommodate backward compatibility, a Suite B IPsec compliant system can be configured to use IKEv1 so long as only IKEv2 is used between a Suite B compliant initiator and responder. However, when IKEv1 is being used, the system is not being operated in a Suite B compliant mode.

IKEv2 does not specify how Identification Payloads (IDi and IDr) in the IKE_AUTH exchanges are used for policy lookup. For Suite B compliant systems, the IKEv2 authentication method MUST NOT use the Identification Payloads for policy lookup. Instead, the authentication method MUST use an end-entity found in the end-entity certificate provided by the authenticating party.

The administrative user interface (UI) for a system that conforms to this profile MUST allow the operator to specify a single suite. If only one suite is specified in the administrative UI, the IKEv2 implementation MUST only offer algorithms for that one suite.

The administrative UI MAY allow the operator to specify more than one suite; if it allows this, it MUST allow the operator to specify a preferred order for the suites that are to be offered or accepted. The preferred order MUST follow the direction provided in Section 4. If more than one suite is specified in the administrative UI, the IKEv2 implementation MUST only offer algorithms for those suites.

9. Security Considerations

This document discusses security requirements throughout, and it inherits the security considerations of [RFC4303], [RFC4754], [RFC5759], and [RFC5996].

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4754] Fu, D. and J. Solinas, "IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)", RFC 4754, January 2007.

[RFC5759] Solinas, J. and L. Zieglar, "Suite B Certificate and Certificate Revocation List (CRL) Profile", RFC 5759, January 2010.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

[RFC6379] Law, L. and J. Solinas, "Suite B Cryptographic Suites for IPsec", RFC 6379, October 2011.

[FIPS180-3] National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-3, October 2008.

[FIPS186-3] National Institute of Standards and Technology, "Digital Signature Standard (DSS)", FIPS PUB 186-3, June 2009.

[FIPS197] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", FIPS PUB 197, November 2001.

[SP800-56A] National Institute of Standards and Technology, "Recommendation for Pair-wise Key Establishment Schemes Using Discrete Logarithm Cryptography", NIST Special Publication 800-56A, March 2007.

[SP800-57] National Institute of Standards and Technology, "Recommendation for Key Management - Part 1", NIST Special Publication 800-57, March 2007.

10.2. Informative References

[IKEV2IANA] "Internet Key Exchange Version 2 (IKEv2) Parameters", <http://www.iana.org>.

[SuiteB] U.S. National Security Agency, "NSA Suite B Cryptography", January 2009, <http://www.nsa.gov/ia/programs/suiteb_cryptography/>.

[RFC5903] Fu, D. and J. Solinas, "Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2", RFC 5903, June 2010.

Authors' Addresses

Kelley W. Burgin
National Security Agency

EMail: kwburgi@tycho.ncsc.mil

Michael A. Peck
The MITRE Corporation

EMail: mpeck@mitre.org