Delay-Tolerant Networking
Internet-Draft
Intended status: Experimental
Expires: July 3, 2016

E. Birrane
JHU/APL

December 31, 2015

Suite B Profile for Bundle Protocol Security (BPSec)
draft-birrane-dtn-bpsec-suiteb-profile-00

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 with Bundle Protocol Security (BPSec).

Since many of the Suite B algorithms enjoy uses in other environments as well, 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 details repeated to aid developers that choose to support Suite B within BPSec.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document specifies the conventions for using NSA Suite B Cryptography [SuiteB] with Bundle Protocol Security (BPSec) [I-D.ietf-dtn-bpsec]. This document is an update to the Suite-B profile created by Burgin and Hennessy [I-D.hennessy-bsp-suiteb-profile]. This update adapts the profile from BSP [RFC6257] to BPSec.

BPSec provides source authentication, data integrity, and data confidentiality services for the Bundle Protocol (BP) [RFC5050].

[I-D.birrane-dtn-bpsec-suiteb-ciphersuites] defines ciphersuites for BPSec that are comprised of Suite B algorithms for use with the security block types BAB, BIB, and BCB. Suite B compliant implementations for BPSec MUST use one of these ciphersuites, depending upon the desired security level and security services.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "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) [FIPS197] (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 sake of clarity, we list both names below.

Curve	NIST Name	SECG Name	OID [FIPS186-3]
P-256	nistp256	secp256r1	1.2.840.10045.3.1.7
P-384	nistp384	secp384r1	1.3.132.0.34

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
Key Wrap	AES-128 Key Wrap	AES-256 Key Wrap
Hash for PRF/MAC	SHA-256	SHA-384

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, with Column 1 being the preferred suite.

At the 192-bit minimum level of security:

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

4.2. Suite B Authentication

Digital signatures using ECDSA MUST be used for authentication by Suite B compliant BPSec implementations. To simplify notation, ECDSA- 256 will be used to represent an instantiation of the ECDSA algorithm using the P-256 curve and the SHA-256 hash function, and ECDSA-384 will be used to represent 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 Suite B compliant BPSec implementation MUST use either ECDSA-256 or ECDSA-384 for authentication. It is allowable for one party to authenticate with ECDSA-256 and the other party to authenticate with ECDSA-384.

Security-aware nodes in a Suite B compliant BPSec implementation 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 unless it is absolutely certain that the implementation will never need to verify certificates from an authority which uses an ECDSA-384 signing key.

Security-aware nodes in a Suite B compliant BPSec implementation configured at a minimum level of security of 192 bits MUST use ECDSA-384 for authentication and MUST be able to verify ECDSA-384 signatures.

4.3. Digital Signatures and Certificates

Security-aware nodes in a Suite B compliant BPSec implementation, 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 field set for digital signature. The endpoint IDs MUST be placed in the subjectAltName field of the X.509 certificate.

5. Suite B Ciphersuites

Each system MUST specify a security level of a minimum of 128 bits or 192 bits. The security level determines which suites from [I-D.birrane-dtn-bpsec-suiteb-ciphersuites] are allowed.

Each of the ciphersuites specified in [I-D.birrane-dtn-bpsec-suiteb-ciphersuites] satisfy the Suite B requirements in Section 3 of this document.

At the 128-bit minimum level of security:

> If a Block Integrity Block (BIB) is included in the bundle, one of BIB-ECDSA-SHA256 or BIB-ECDSA-SHA384 MUST be used by Suite B compliant BPSec implementations.
>
> If a Block Confidentiality Block (BCB) is included in the bundle, one of BCB-ECDH-SHA256-AES128 or BCB-ECDH-SHA384-AES256 MUST be used by Suite B compliant BPSec implementations.

At the 192-bit minimum level of security:

> If a Block Integrity Block (BIB) is included in the bundle, BIB-ECDSA-SHA384 MUST be used by Suite B compliant BPSec implementations.
>
> If a Block Confidentiality Block (BCB) is included in the bundle, BCB-ECDH-SHA384-AES256 MUST be used by Suite B compliant BPSec implementations.

6. Security Considerations

Two levels of security may be achieved using this specification. Users must consider their risk environment to determine which level is appropriate for their own use.

This specification does not consider the CMS Block of the BPSec specification. Details for using CMS in Suite B can be found in

[RFC6318]. The security considerations in [RFC5652] discuss the CMS as a method for digitally signing data and encrypting data.

7. IANA Considerations

None.

8. References

8.1. Normative References

[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.

[I-D.birrane-dtn-bpsec-suiteb-ciphersuites]
Birrane, E., "Suite B Ciphersuites for Bundle Protocol Security (BPSec)", draft-birrane-dtn-bpsec-suiteb-ciphersuites-00 (work in progress), December 2015.

[I-D.ietf-dtn-bpsec]
Birrane, E., Pierce-Mayer, J., and D. Iannicca, "Bundle Protocol Security Specification", draft-ietf-dtn-bpsec-00 (work in progress), December 2015.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <http://www.rfc-editor.org/info/rfc5652>.

[RFC5759] Solinas, J. and L. Zieglar, "Suite B Certificate and Certificate Revocation List (CRL) Profile", RFC 5759, DOI 10.17487/RFC5759, January 2010, <http://www.rfc-editor.org/info/rfc5759>.

[RFC6318] Housley, R. and J. Solinas, "Suite B in Secure/ Multipurpose Internet Mail Extensions (S/MIME)", RFC 6318, DOI 10.17487/RFC6318, June 2011, <http://www.rfc-editor.org/info/rfc6318>.

8.2. Informative References

[I-D.hennessy-bsp-suiteb-ciphersuites] Burgin, K. and A. Hennessy, "Suite B Ciphersuites for the Bundle Security Protocol", draft-hennessy-bsp-suiteb-ciphersuites-00 (work in progress), March 2012.

[I-D.hennessy-bsp-suiteb-profile] Burgin, K. and A. Hennessy, "Suite B Profile for the Bundle Security Protocol", draft-hennessy-bsp-suiteb-profile-00 (work in progress), March 2012.

[RFC5050] Scott, K. and S. Burleigh, "Bundle Protocol Specification", RFC 5050, DOI 10.17487/RFC5050, November 2007, <http://www.rfc-editor.org/info/rfc5050>.

[RFC6257] Symington, S., Farrell, S., Weiss, H., and P. Lovell, "Bundle Security Protocol Specification", RFC 6257, DOI 10.17487/RFC6257, May 2011, <http://www.rfc-editor.org/info/rfc6257>.

[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.

[SuiteB] U.S. National Security Agency, "Fact Sheet NSA Suite B Cryptography", NIST Special Publication 800-56A, January 2009, <http://www.nsa.gov/ia/programs/suiteb_cryptography/>.

Author's Address

Edward J. Birrane
The Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Rd.
Laurel, MD 20723
US

Phone: +1 443 778 7423
Email: Edward.Birrane@jhuapl.edu