Delay-Tolerant Networking
Internet-Draft
Intended status: Standards Track
Expires: September 6, 2018

E. Birrane
JHU/APL

March 5, 2018

BPSec Interoperability Cipher Suites
draft-birrane-dtn-bpsec-interop-cs-01

Abstract

This document defines a set of integrity and confidentiality cipher suites suitable for testing the interoperability of Bundle Protocol Security (BPSec) implementations.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 6, 2018.

Table of Contents

1. Introduction

The Bundle Protocol Security (BPSec) [I-D.ietf-dtn-bpsec] specification provides inter-bundle integrity and confidentiality features for networks deploying the Bundle Protocol (BP) [I-D.ietf-dtn-bpbis]. BPSec defines a set of BP extension blocks to carry cipher suite results and associated meta-data, but does not define a common set of supported cipher suites.

This document defines an integrity cipher suite and a confidentiality cipher suite suitable for populating BPSec Block Integrity Blocks (BIBs) and Block Confidentiality Blocks (BCBs), respectively.

This purpose of the cipher suites described in this document is twofold. First, these suites should be used to test the interoperability of BPSec implementations. Second, this specification can serve as a template to be followed by other BPSec cipher suite authors.

The intent of these cipher suite definitions is to provide a mechanism for interoperability testing. There is no claim that these cipher suites are suitable for operational deployment in any particular networking scenario. Further, there is no requirement that these cipher suites be used in any operational network deployments.

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. Cipher Suite BIB-HMAC256-SHA256

3.1. Overview

This integrity cipher suite provides a signed hash over the security target based on the use of the SHA-256 message digest algorithm [RFC4634] combined with HMAC [RFC2104] with a 256 bit truncation length. This formulation is based on the HMAC 256/256 algorithm defined in [COSE] Table 7: HMAC Algorithm Values.

The BIB-HMAC256-SHA256 ciphersuite has ciphersuite ID value 0x01.

3.2. Key Considerations

Keys used with this specification MUST be symmetric and 256 bits in length.

This cipher suite provides no requirements on the configuration or management of keys.

3.3. Canonicalization Algorithms

BIB-HMAC256-SHA256 uses the standard canonicalization algorithms defined in BPSec and operates over the entire contents of the security target data block. This cipher suite does not include hashing over other parts of the target block header, such as the block type and block length.

3.4. Cipher Suite Parameter Definitions

BIB-HMAC256-SHA256 defines the following cipher suite parameters.

BIB-HMAC256-SHA256 Parameters

Parm Id	Parm Name	CBOR Type	Description
1	Key	byte string (major type 2)	Material encoded or protected by the key management system and used to transport an ephemeral key protected by a long-term key.

Table 1

3.5. Security Result Definitions

BIB-HMAC256-SHA256 defines the following security results.

BIB-HMAC256-SHA256 Security Results

Result Id	Result Name	CBOR Type	Description
1	Tag	byte string (major type 2)	The tag produced by HMAC.

Table 2

4. Cipher Suite BCB-AES-GCM-128

4.1. Overview

This confidentiality cipher suite provides cipher text to replace the data contents of the target block using the AES cipher operating in GCM mode [AES-GCM]. This formulation is based on the A128GCM algorithm defined in [COSE] Table 9: Algorithm Value for AES-GCM.

The BCB-AES-GCM-128 ciphersuite has ciphersuite ID value 0x02.

4.2. Key Considerations

Keys used with this specification MUST be symmetric and 128 bits in length.

This cipher suite provides no requirements on the configuration or management of keys.

4.3. Canonicalization Algorithms

BCB-AES-GCM-128 uses the standard canonicalization algorithms defined in BPSec and operates over the entire contents of the security target data block. This cipher suite does not include encryption over other parts of the target block header, such as the block type and block length.

4.4. Cipher Suite Parameter Definitions

BCB-AES-GCM-128 defines the following cipher suite parameters. It should be noted in this specification there is no additional authenticated data passed in to the AES-GCM cipher. The plaintext is the only data input and MUST be the entire data contents of the target block.

BCB-AES-GCM-128 Parameters

Parm Id	Parm Name	CBOR Type	Description
1	Key	byte string (major type 2)	Material encoded or proteted by the key management system and used to transport an ephemeral key protected by a long-term key.
2	Initialization Vector	byte string (major type 2)	The initialization vector. A random value between 8-16 bytes. 12 bytes is recommended.

Table 3

4.5. Security Result Definitions

BCB-AES-GCM-128 defines the following security results. It should be noted that cipher text is not a security result as the resultant cipher text is stored in the target block. When operating in GCM mode, AES produces cipher text of the same size as its plain text and, therefore, no security results are necessary to capture padding information.

BCB-AES-GCM-128 Security Results

Result Id	Result Name	CBOR Type	Description
1	Authentication Tag	byte string (major type 2)	Output from the AES-GCM cipher. This value MUST be 16 bytes long.

Table 4

5. IANA Considerations

5.1. Bundle Block Types

This specification allocates two block types from the "BPSec Cipher Suite IDs" registry defined in [I-D.ietf-dtn-bpsec].

Additional BPSec Cipher Suite IDs:

Value	Description	Reference
1	BIB-HMAC256-SHA256	This document
2	BCB-AES-GCM-128	This document

Table 5

6. Normative References

[AES-GCM] Dworkin, M., "NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.", November 2007.

[COSE] Schaad, J., "CBOR Object Signing and Encryption (COSE)", draft-ietf-cose-msg-24 (work in progress), November 2016.

[I-D.ietf-dtn-bpbis] Burleigh, S., Fall, K., and E. Birrane, "Bundle Protocol Version 7", draft-ietf-dtn-bpbis-10 (work in progress), November 2017.

[I-D.ietf-dtn-bpsec]
Birrane, E. and K. McKeever, "Bundle Protocol Security Specification", draft-ietf-dtn-bpsec-06 (work in progress), October 2017.

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997, <https://www.rfc-editor.org/info/rfc2104>.

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

[RFC4634] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and HMAC-SHA)", RFC 4634, DOI 10.17487/RFC4634, July 2006, <https://www.rfc-editor.org/info/rfc4634>.

Author's Address

Edward J. Birrane, III
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