Delay-Tolerant Networking
Internet-Draft
Intended status: Standards Track
Expires: September 12, 2019

E. Birrane
JHU/APL

March 11, 2019

BPSec Interoperability Security Contexts
draft-ietf-dtn-bpsec-interop-sc-00

Abstract

This document defines an integrity security context and a confidentiality security context 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 12, 2019.

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 security information produced under the auspices of some security context, but does not define a common set of these security contexts.

This document defines two security contexts (one for integrity services and one for confidentiality services) suitable for populating BPSec Block Integrity Blocks (BIBs) and Block Confidentiality Blocks (BCBs).

This purpose of the security contexts described in this document is twofold. First, these contexts should be used to test the interoperability of BPSec implementations. Second, this

specification can serve as a template to be followed by other BPSec security context authors.

The intent of these security context definitions is to provide a mechanism for interoperability testing. There is no claim that these

contexts are suitable for operational deployment in any particular networking scenario. Further, there is no requirement that these contexts be used in any operational network deployments.

These contexts generate information that MUST be encoded using the CBOR specification documented in [RFC7049].

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. Security Context BIB-HMAC256-SHA256

3.1. Overview

This integrity context 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 [RFC8152] Table 7: HMAC Algorithm Values.

The BIB-HMAC256-SHA256 context has a Security Context ID of 0x1.

3.2. Key Considerations

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

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

3.3. Canonicalization Algorithms

BIB-HMAC256-SHA256 uses the standard canonicalization algorithms defined in [I-D.ietf-dtn-bpsec] and operates over all of the block-type-specific data fields for the security target. This context does not include hashing over other parts of the target block header, such as the block type code, block number, block processing control flags, or any CRC information.

3.4. Security Context Parameter Definitions

BIB-HMAC256-SHA256 defines the following security context parameters.

BIB-HMAC256-SHA256 Parameters

Parm Id	Parm Name	CBOR Type	Description
1	Key	byte string	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	The tag produced by HMAC.

Table 2

4. Security Context BCB-AES-GCM-256

4.1. Overview

This confidentiality context provides cipher-text to replace the plain-text block-type-specific data fields of its target block. BCB-AES-GCM-256 uses the Advanced Encryption Standard (AES) cipher operating in Galois/Counter Mode (GCM) [AES-GCM]. This formulation is based on the A256GCM algorithm defined in [RFC8152] Table 9: Algorithm Value for AES-GCM.

The BCB-AES-GCM-256 context has a Security Context ID of 0x02.

This context modifies the size of the target block.

4.2. Key Considerations

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

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

4.3. Canonicalization Algorithms

BCB-AES-GCM-256 uses the standard canonicalization algorithms defined in [I-D.ietf-dtn-bpsec] and operates over all of the block-type-specific data fields for the security target. This context does not include hashing over other parts of the target block header, such as the block type code, block number, block processing control flags, or any CRC information.

4.4. Processing

4.4.1. Encryption

When encrypting, the BCB-AES-GCM-256 context treats the catenation of the target block's block-type-specific data fields as a single set of plain-text.

Cipher-text, once calculated, is stored as a CBOR byte string replacing the value of the target block's block-type-specific data.

Because the plain-text and cipher-text will have the same length, the CBOR byte string encoding will have the same encoding of the byte string type and length. This allows the replacement of plain-text with cipher-text without any additional consideration of block-type-specific data field processing.

4.4.2. Decryption

When decrypting, the target block's block-type-specific field is verified to be only a CBOR byte string. If this is not the case the decryption is treated as failed and processed in accordance with local security policy. Otherwise, the byte string and key information is passed to the cipher for decryption.

If the cipher-text fails to authenticate, or if there are other problems in the decryption (such as the creation of invalid CBOR plain-text) then the decryption MUST be treated as failed and processed in accordance with local security policy.

If the decryption succeeds, the resultant plain-text MUST replace the cipher-text in the target-block.

4.5. Security Context Parameter Definitions

BCB-AES-GCM-256 defines the following security context parameters. It should be noted in this specification there is no additional authenticated data passed in to the AES-GCM cipher. The plain-text is the only data input and MUST be the entire data contents of the target block. Because replaying an IV in counter mode voids the confidentiality of all messages encryption with said IV, this context also requires a unique IV for every encryption performed with the same key. This means the same key and IV combination must never be used more than once.

BCB-AES-GCM-256 Parameters

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

Table 3

4.6. Security Result Definitions

BCB-AES-GCM-256 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-256 Security Results

Result Id	Result Name	CBOR Type	Description
1	Authentication Tag	byte string	Output from the AES-GCM cipher. This value (prior to

			CBOR encoding) MUST be 16 bytes long.

Table 4

5. IANA Considerations

5.1. Bundle Block Types

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

Additional BPSec Security Context IDs:

Value	Description	Reference
1	BIB-HMAC256-SHA256	This document
2	BCB-AES-GCM-256	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.

[I-D.ietf-dtn-bpbis] Burleigh, S., Fall, K., and E. Birrane, "Bundle Protocol Version 7", draft-ietf-dtn-bpbis-12 (work in progress), November 2018.

[I-D.ietf-dtn-bpsec] Birrane, E. and K. McKeever, "Bundle Protocol Security Specification", draft-ietf-dtn-bpsec-09 (work in progress), February 2019.

[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>.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object
Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049,
October 2013, <https://www.rfc-editor.org/info/rfc7049>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)",
RFC 8152, DOI 10.17487/RFC8152, July 2017,
<https://www.rfc-editor.org/info/rfc8152>.

Appendix A. Acknowledgements

The following participants contributed useful analysis of this specification: Prathibha Rama of the Johns Hopkins University Applied Physics Laboratory.

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