JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

BPSec Default Security Contexts Update

IETF-109

Ken McKeever
Ken.McKeever@jhuapl.edu
240-228-2237

Summary of Updates

- In ietf-dtn-bpsec-interop-sc-02, the security contexts have been updated for greater flexibility and specificity

- Adds detail to security contexts BIB-HMAC-SHA2 and BCB-AES-GCM

- Added:
  - Support for multiple key lengths as a security context parameter
  - Definition of security context scope to identify input information
  - Canonicalization algorithms for inputs
  - New security context parameters

Support for Multiple Key Lengths

- The key length is now parameterized in the default security contexts
  - Streamline the definition of similar security contexts

- For BIB-HMAC-SHA2:
  - HMAC256/SHA256 as defined in [RFC8152] Table 7: HMAC Algorithm Values
  - HMAC384/SHA384 as defined in [RFC8152] Table 7: HMAC Algorithm Values
  - HMAC512/SHA512 as defined in [RFC8152] Table 7: HMAC Algorithm Values

- For BCB-AES-GCM:
  - A128GCM as defined in [RFC8152] Table 9: Algorithm Values for AES-GCM
  - A192GCM as defined in [RFC8152] Table 9: Algorithm Values for AES-GCM
  - A256GCM as defined in [RFC8152] Table 9: Algorithm Values for AES-GCM

Security Context Scope

- The scope refers to the set of information used as input to produce an output for the security operation

- Primary block
  - The primary block identifies a bundle and, once created, the contents of this block are immutable. Changes to the primary block associated with the security target indicate that the security target (and BIB/BCB) may no longer be in the correct bundle.

- Security target other fields
  - The other fields of the security target include block identification and processing information. Changing this information changes how the security target is treated by nodes in the network even when the "user data" of the security target are otherwise unchanged.

- BIB/BCB other fields
  - The other fields of the BIB/BCB include block identification and processing information. Changing this information changes how the BIB/BCB is treated by nodes in the network, even when other aspects of the BIB/BCB are unchanged.

BIB-HMAC-SHA2 Input Canonicalization Algorithm

- The BIB-HMAC-SHA2 security context defines a canonicalization algorithm for the Integrity Protected Plain Text (IPPT)
  - Appends canonical forms of components of the bundle specified by the Integrity Scope Parameters

The IPPT is constructed using the following process.

1. The canonical form of the IPPT starts as the empty set with length 0.

2. If the Integrity Scope parameter is present and the Primary Block Flag is set to 1, then a canonical form of the bundle's primary block MUST be calculated and the result appended to the IPPT.

3. If the Integrity Scope parameter is present and the Security Header flag is set to 1, then the canonical form of the Block Type Code, Block Number, and Block Processing Control Flags associated with the BIB MUST be calculated and, in that order, appended to the IPPT.

4. If the Integrity Scope parameter is present and the Target Header flag is set to 1, then the canonical form of the Block Type Code, Block Number, and Block Processing Control Flags associated with the security target MUST be calculated and, in that order, appended to the IPPT.

5. The canonical form of the security target block-type-specific data MUST be calculated and appended to the IPPT.

BCB-AES-GCM Input Canonicalization Algorithms

- The BCB-AES-GCM security context defines canonicalization algorithms for
  - The plaintext used during encryption
    - The plain text used during encryption MUST be calculated as the single, definite-length CBOR byte string representing the block-type-specific data field of the security target excluding the CBOR byte string identifying byte and optional CBOR byte string length field.
  - The ciphertext used during decryption
    - The cipher text used during decryption MUST be calculated as the single, definite-length CBOR byte string representing the block-type-specific data field excluding the CBOR byte string identifying byte and optional CBOR byte string length field.
  - The Additional Authenticated Data (AAD)
    - Appends canonical forms of components of the bundle specified by the AAD Scope Parameters
    - The algorithm is similar to the canonicalization algorithm for the BIB-HMAC-SHA2 IPPT

Updated Security Context Parameters

- Provides the following parameters to the BIB-HMAC-SHA2 context:
  - SHA Variant
  - Encapsulated Key
  - Integrity Scope Flags
    - Primary Block
    - Target Header
    - Security Header

- Provides the following parameters to the BCB-AES-GCM context:
  - Initialization Vector *(already present in -01)*
  - Key Length
  - Encapsulated Key
  - AAD Scope Flags
    - Primary Block
    - Target Header
    - Security Header

APL

JOHNS HOPKINS

APPLIED PHYSICS LABORATORY