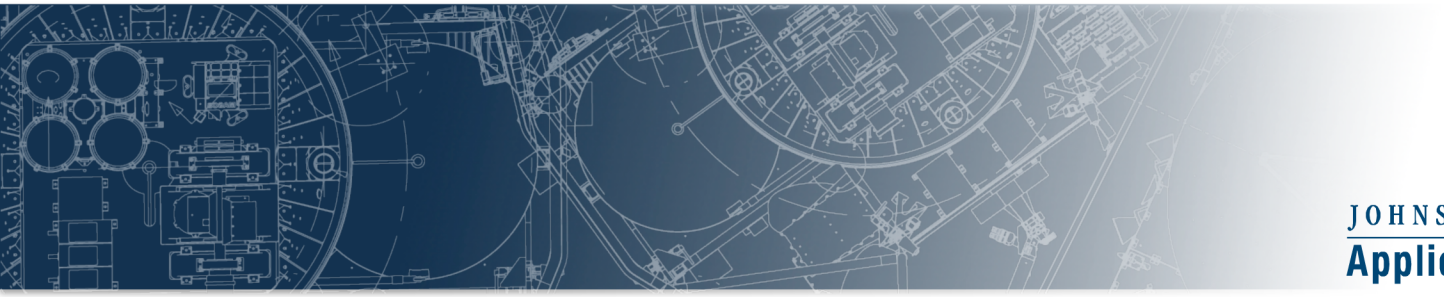
BPSEC Updates
draft-ietf-dtn-bpsec-06

IETF 100

Edward Birrane
Edward.Birrane@jhuapl.edu
443-778-7423



JOHNS HOPKINS UNIVERSITY
Applied Physics Laboratory

Overview

- Summary
- Updates
- Outstanding Comments
- Interoperability Cipher Suites
- Next Steps

Brief Summary

- Motivation for this document
  - In-bundle security mechanism is needed in some cases
  - If you do not want in-bundle security, you can secure BP by having
- Design decisions
  - Different blocks in a bundle can have different security
  - Processing order must be unambiguous at a receiver
  - New cipher suites must be able to be added at future dates
- Syntax
  - Two new extensions blocks defined (BIB, BCB)
  - Block Processing Rules to Enforce Determinism
- Security Considerations
  - Brief review of attacker types in a DTN
  - Explanation for why security policy should be out-of-band configured in the network and not included in the bundle itself.

Updates in version -06

- Responded to comments received from v-05
  - Reduced occurrence of MUST in the document.
  - Corrected a few misspellings.
  - Updated sections in the security analysis section
    - *Clarified the security implication of long-lived bundles in a DTN. There is a subtle difference between a bundle that lives in the network for a very long time and a packet that lives in the network for a short time but is captured and has payload that is relevant for a long time.*
    - *Corrected flawed assumption that signature substitution is impossible if encrypting signed content. Updated text to require specific type of encryption scheme to protect against that instance.*

Outstanding Items/Comments

- Section 3.6 – Security Block Format
  - The document specifies a key-value format for representing
    - *Cipher Suite Parameters*
    - *Results*
  - The document DOES NOT specify individual items
    - *Specific keys and associated data types of their values*
    - *Required that individual cipher suite specifications list parameters and formats of results.*
    - *Recommended that existing standards be used for these wherever possible.*
  - Open comment: Should BPSEC require a key-value syntax or treat cipher suite parameters as an opaque blob passed to cipher suite implementations?
    - *Initial thought: No. May have implications on interoperability or processing.*
    - *If needed, cipher suite could define single key "opaque data:" and achieve same result.*

Outstanding Items/Comments

- BPSec cannot be submitted until BPBis is finalized
  - From mailing list: concern that any changes to Bpbis during standardization will require rework of BpSec.
  - Disagree because the coupling between BPSec and Bpbis is not significant in meaningful areas.
    - *BPSec information will be stored in Bundle Extension Blocks. While block formats may change, as long as extension blocks exist BPSec is unchanged in this regard. BPSec referenced BPBis for block formatting.*
    - *BPSec requires concept of an extension block identifier. This is believed to be an area of Bpbis where change is extremely unlikely.*
    - *Behavioral changes to Bpbis will affect security policy, but security policy and key management are outside the scope of this document.*

Outstanding Items/Comments

- BPSec has older references to Bpbis document
  - References expected to be updated through the review process?

Outstanding Items/Comments

- BPSec must define interoperability Cipher Suites
  - Agreed. Publish as a separate document.
    - *AFTER Bpsec in last call: changes to BpSec could change cipher suite definitions document.*
    - *Draft at:* ***draft-birrane-dtn-bpsec-interop-cs-00***
  - Integrity Cipher Suite
    - *BIB-HMAC256-SHA256*
      - The 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.
  - Confidentiality Cipher Suite
    - *BCB-AES-GCM-128*
      - The 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.

Next Steps

- BPSEC
  - No significant problems with BPSec have been identified.
    - *Received reviews within community*
    - *Requested reviews: NIST, Security ADs.*

- Interoperability Cipher Suites
  - Need a short period of review and updates.
  - Waiting for BPSec to go forward.

Thank you!

Questions/Comments

Thank you!

Backup Slides

Summary (1/3)

- Motivation for this document
  - In-bundle security mechanism is needed in some cases
    - *Different blocks may have different security needs*
    - *Different nodes may impose different security policy*
  - If you do not want in-bundle security, you can secure BP by having
    - *Users protect their data at the application layer (e.g. secure payload)*
    - *Users select secure convergence layers (if they exist)*

- Design decisions
  - Different blocks in a bundle can have different security
  - Processing order must be unambiguous at a receiver
  - New cipher suites must be able to be added at future dates

Summary (2/3)

- Block Format
  - Two new extensions blocks defined
    - *Both capture list of targets they act upon, key information, cipher suite configuration, and result information.*
    - *Integrity (BIB) – Holds signature*
    - *Confidentiality (BCB) – Indicates target(s) have had their block data replaced with crypto-text*
  - A security block can target 1 or more other blocks
    - *Multiple targets prevents redundant info in the bundle.*
  - Mechanism provided to add new security blocks in other documents if necessary.
- Block Processing Rules to Enforce Determinism
  - If a BCB target is encrypted, a BIB on that target is also encrypted.
  - A BIB cannot target a BCB or a block protected by a BCB.
    - *There exist BCB cipher suites that also generate integrity signatures*
  - At a receiver, BCBs must be processed before BIBs.

Summary (3/3)

- Block Processing (cont)
  - Cannot add BIBs and BCBs if bundle represents a fragment.
    - *Can encapsulate in that case.*
  - Nodes determine if they are a security destination by policy.
    - *Dangerous and confusing to have bundle assert internal to itself what the security destination would be.*
- Security Considerations
  - Brief review of attacker types in a DTN, explaining how to apply BCB and BIB in these cases.
  - Explanation for why security policy should be out-of-band configured in the network and not included in the bundle itself.
    - *Namely, a bundle might have blocks dropped by a malicious BPA, so blocks that encode security requirements cannot be relied on.*