Updated SBSP
draft-birrane-dtn-sbsp-01.txt

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

JOHNS HOPKINS UNIVERSITY
Applied Physics Laboratory

SBSP - Added Key Properties

- Fundamental
  - End-to-end confidentiality
  - End-to-end integrity
  - Multiple ciphersuite support

- Additional
  - Block-Level Granularity
  - Multiple Security Sources
  - Single Security Destinations
  - Mixed Security Policy
  - User-selectable ciphersuites / Configurable policy
  - Deterministic Processing

SBSP - Key Properties 1

- Block-Level Granularity
  - Security services applied to blocks, not bundles.
    - *Integrity sign extension block 1*
    - *Encrypt payload block*

- Multiple Security Sources
  - BPAs can apply security to both transmitted and forwarded bundles.
    - *Bundle source adds an integrity signature to the payload. Then a gateway node adds encryption.*

- Single Security Destination
  - Completely decouple routing and security.
    - *Use tunneling (BIBE) for cases where an “intermediate destination” is necessary.*

SBSP - Key Properties 2

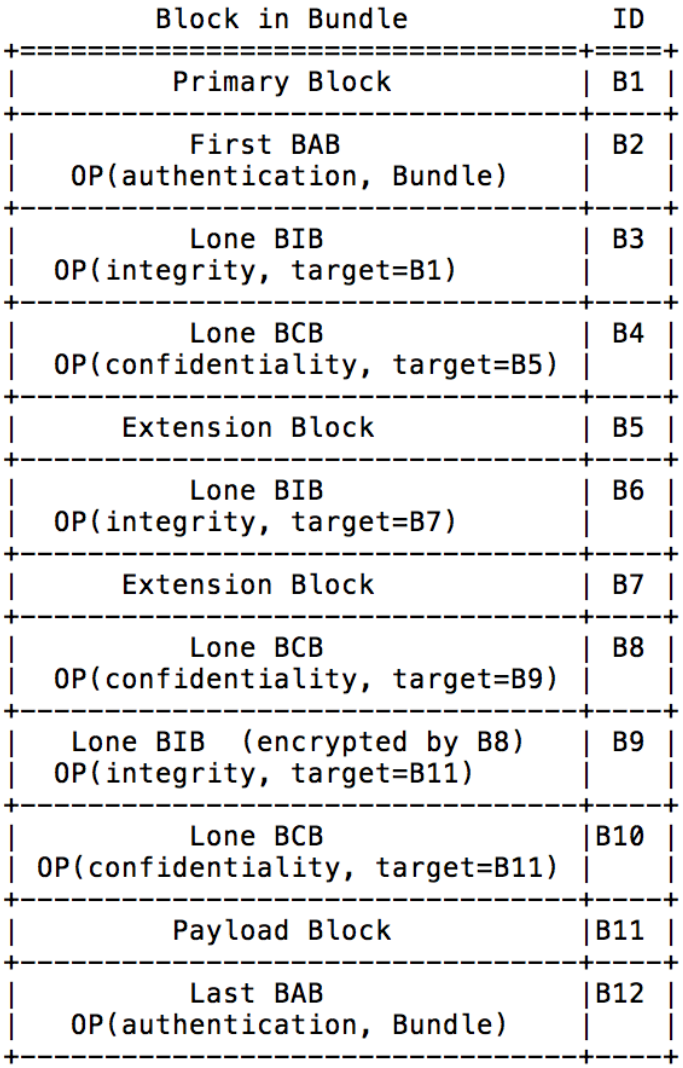
- Mixed Security Policy
  - Waypoints must be able to process an integrity-protected block without having the keys to verify the integrity.
  - Non-security nodes must be accommodated in the network.

- User-Selected Ciphersuites
  - Encoding of ciphersuite identifiers and parameters

- Deterministic Processing
  - Security services are not applied to fragments.
    - *Wrap a fragment in a new bundle through BIBE if it needs security services.*
  - Carefully specify interaction between confidentiality and integrity when they are separate services.

SBSP Block Structure

- SBSP blocks added 1 per security service
  - SBSP block is a tuple of (security service, security target).
- Fits key properties
  - Waypoints can add SBSP blocks
  - Different ciphersuites/services can be applied to different targets.
  - Deterministic rules for processing BIB and BCB blocks.
- Reference implementation emerging
  - ION 3.4.x
  - SBSP captures simple cases of RFC6257. Not hard to port.



```
             Block in Bundle                 ID
+==================================+====+
|          Primary Block           | B1 |
+----------------------------------+----+
|            First BAB             | B2 |
|   OP(authentication, Bundle)     |    |
+----------------------------------+----+
|            Lone BIB              | B3 |
|  OP(integrity, target=B1)        |    |
+----------------------------------+----+
|            Lone BCB              | B4 |
|  OP(confidentiality, target=B5)  |    |
+----------------------------------+----+
|        Extension Block           | B5 |
+----------------------------------+----+
|            Lone BIB              | B6 |
|  OP(integrity, target=B7)        |    |
+----------------------------------+----+
|        Extension Block           | B7 |
+----------------------------------+----+
|            Lone BCB              | B8 |
|  OP(confidentiality, target=B9)  |    |
+----------------------------------+----+
|   Lone BIB  (encrypted by B8)    | B9 |
|  OP(integrity, target=B11)       |    |
+----------------------------------+----+
|            Lone BCB              |B10 |
| OP(confidentiality, target=B11)  |    |
+----------------------------------+----+
|          Payload Block           |B11 |
+----------------------------------+----+
|            Last BAB              |B12 |
|   OP(authentication, Bundle)     |    |
+----------------------------------+----+
```

SBSP - Added CMS Block

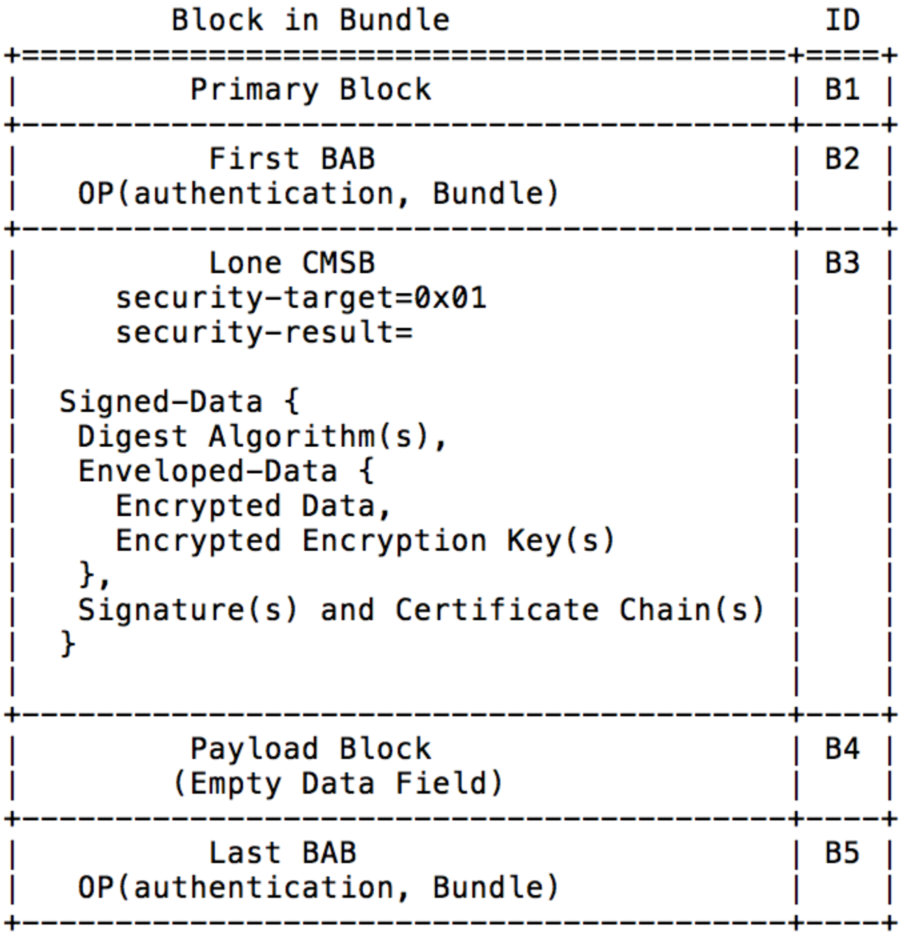
- NASA/GRC and DLR provided initial text
  - Case where payload is CMS text not in scope for this spec
    - *That is application-layer security.*

- Changes to the Abstract Security Block
  - Ciphersuite ID and flags in the ASB are now optional
    - *CMS text in the CMS Block captures this in the block payload.*

- Updated processing rules
  - CMS Block and BCB/BIB cannot share security targets.
  - CMS Block may capture multiple security services for its target.

SBSP - Added CMS Block

- CMS and other blocks can syntactically co-exist in a bundle.
- CMS blocks have option to fully encapsulate targets
  - In example, Lone CMSB (B3) encapsulates the payload.
  - Payload left in place, but with empty data field.
- Option to have CMSB not encapsulate targets as well.



```
              Block in Bundle                           ID
+==========================================+====+
|             Primary Block                |  B1  |
+------------------------------------------+----+
|               First BAB                  |  B2  |
|    OP(authentication, Bundle)            |      |
+------------------------------------------+----+
|               Lone CMSB                  |  B3  |
|      security-target=0x01                |      |
|      security-result=                    |      |
|                                          |      |
|   Signed-Data {                          |      |
|    Digest Algorithm(s),                  |      |
|    Enveloped-Data {                      |      |
|      Encrypted Data,                     |      |
|      Encrypted Encryption Key(s)         |      |
|    },                                    |      |
|    Signature(s) and Certificate Chain(s) |      |
|   }                                      |      |
|                                          |      |
+------------------------------------------+----+
|             Payload Block                |  B4  |
|          (Empty Data Field)              |      |
+------------------------------------------+----+
|               Last BAB                   |  B5  |
|    OP(authentication, Bundle)            |      |
+------------------------------------------+----+
```

SBSP - Open Questions (1/2)

- Do we need an authentication block (BAB)?
  - Authentication at the link layer is considered a GoodThing.
  - Value of authenticating between adjacent hops in the overlay?
  - Proposal 1:
    - *Keep BABs, require policy that has security-aware node process BAB and non-security aware nodes drop bundle or block as per Bundle Protocol block processing flags.*
  - Proposal 2:
    - *Remove BABs and have authentication done by CLA or below.*
- Can blocks encapsulate other blocks?
  - If block B1 encrypts block B2 we have:
  - Proposal 1
    - *Have two blocks: B1 with info and B2 with ciphetext in its payload*
  - Proposal 2
    - *Have 1 block: B1 with info and no record of B2 otherwise in the bundle.*

SBSP - Open Questions (1/2)

- Do we need CMS?
  - Is CMS syntax enabling based on likely adoption, or hindering based on bit size and additional processing/memory requirements?
  - Proposal 1:
    - *Remove CMS from SBSP and let applications tunnel CMS in payloads.*
  - Proposal 2:
    - *Define a CMS block and integrate it into SBSP*
  - Proposal 3:
    - *Modify BAB, BIB, BCB to optionally have CMS in their payloads.*

- What is the correct processing order when layering BIB/BCB?
  - Proposal 1: BCB then BIB
  - Proposal 2: BIB then BCB

Future Work

- Can we re-name SBSP BSP
  - Potential naming collision with RFC6257 (experimental spec from DTN IRTF)
  - SBSP is not a long-term name.
  - Recommend: Rename SBSP as BSP going forward.

- Can we adopt BSP in the DTNWG?

- Other items?