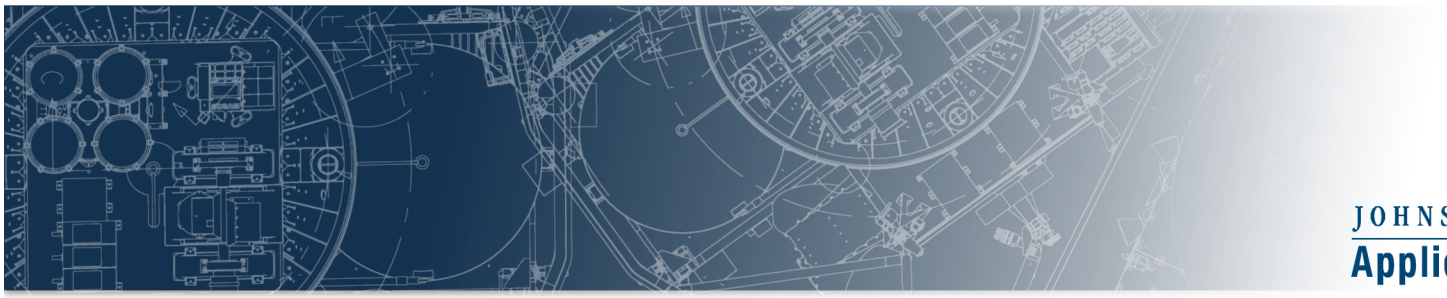
“Streamlined” Bundle Security Protocol

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



JOHNS HOPKINS UNIVERSITY
Applied Physics Laboratory

Overview

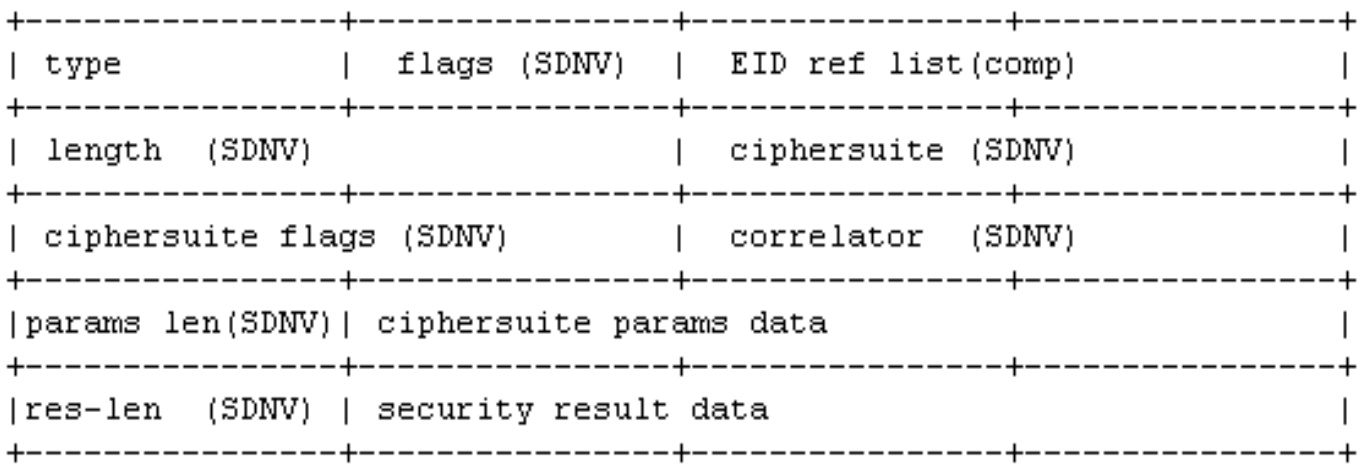
- **Introduction**
  - RFC6257 overview
- **Motivation**
  - Lessons Learned from BSP Implementations
  - Bundle Encapsulation
  - Recommended strategy to capture DTN security mechanisms
- **SBSP Overview**
  - Security Operations Overview
  - New Features and Constraints
- **Security Functions**
  - Review Common Cases
- **Questions**

Bundle Security Protocol Overview

- Defines 4 Extension Blocks (BAB, PIB, PCB, ECB)
  - *Bundle Authentication*: Covers entire bundle
  - *Payload Integrity*: Integrity signature of payload-related blocks
  - *Payload Confidentiality*: Crypto-text of other payload-related blocks, or describes crypto-text residing in payload block.
  - *Extension Security*: Security for non-payload-related blocks.
- May have multiple blocks for a single service
  - Often a pre-payload block working with a post-payload block.
  - Example: Bundle Authentication of a large bundle
- Ciphersuites populate blocks
  - BSP blocks contain ciphersuite identifiers and associated information.
  - Bundle agents expected to support multiple ciphersuites.
- Protocol does not address management issues
  - Key management is an open problem.
  - Security policy enforcement and configuration is an open area.

BSP: Abstract Block Structure

All BSP Blocks follow a standard block structure

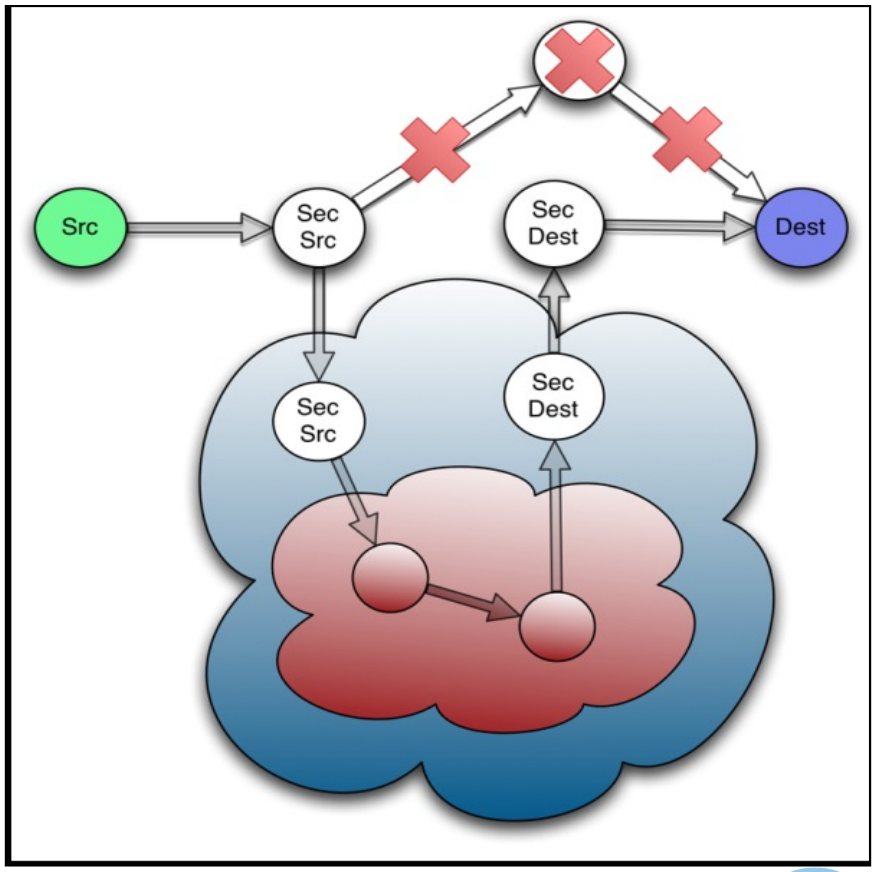


- Software implements this structure and uses it for processing
- When creating/forwarding bundles, structure is populated and then serialized into the bundle bitstream.
- When receiving a bundle, bitstream is desearialized into this structure and then validated.
- Some fields omitted based on whether 1 or 2 blocks are used to implement a security service.

Security Source/Destinations

Each security block has a security source and destination

- Layered Security
  - Security-sources may differ from the bundle source.
  - Security-destinations may differ from the bundle destination.
- Caveats
  - Up to the security-aware node to ensure there are no conflicts amongst all security-destinations in all security blocks in the bundle.
  - Cannot reach the bundle destination before reaching all necessary security-destinations.



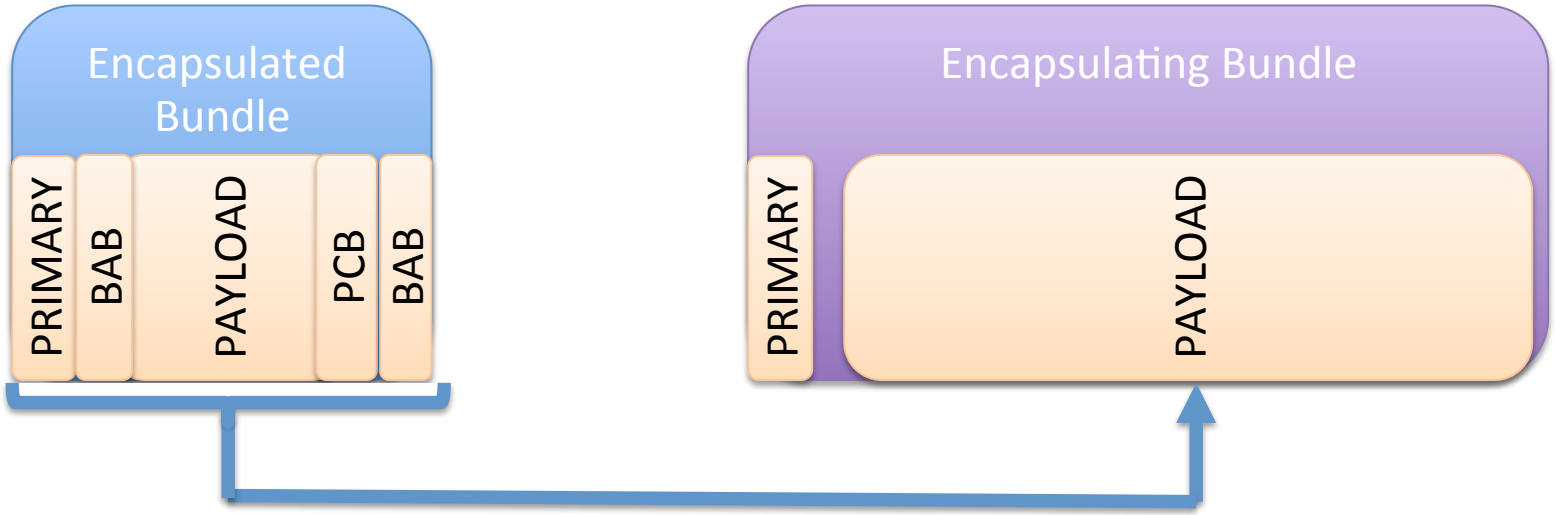
Major Lessons Learned from RFC6257

- Decouple the routing and security functions
  - Security-destinations separate from bundle destinations problematic in many deployment scenarios.
- Make common cases simpler; allow rare cases to scale.
  - Simplify block encapsulation an nesting rules.
- Increase support for non-payload integrity
  - RFC6257 has no integrity mechanism for extension blocks separate from integrity signatures computed as part of confidentiality.
- Leverage encapsulation to simplify processing rules.
  - Require fewer nested security blocks to provide super-encryption
  - Support security tunnels without any changes to the security spec.
- Fragmentation must be addressed more thoroughly
  - Several problematic cases when assembling/fragmenting.

APL

Bundle-in-Bundle Encapsulation

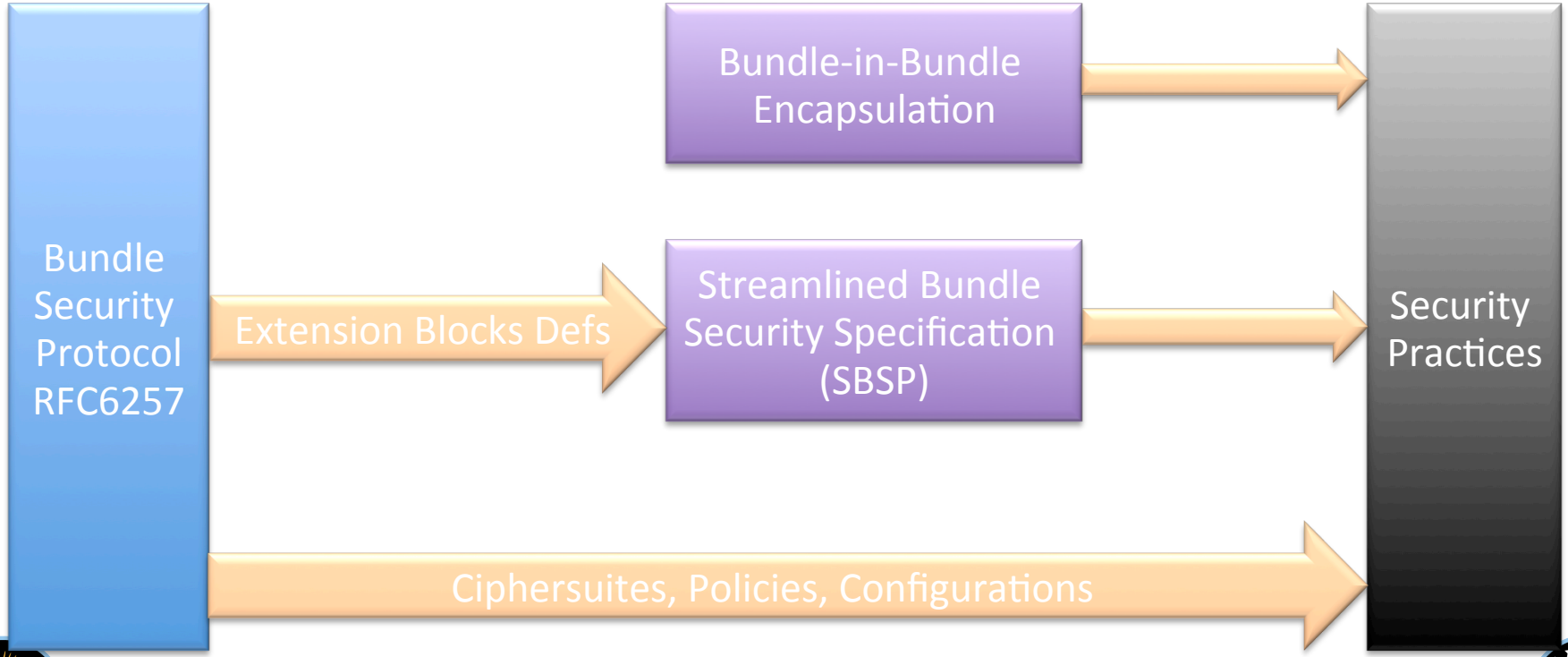
Make an entire bundle the payload of another bundle.



- Implements security tunnels in a graceful way
  - Encapsulated bundle source/destination never changes.
  - Encapsulating bundle src/dest set to the security-src/security-dest
    - *Lets existing routing mechanisms figure out the routing portion.*
- Provides mechanism for hiding primary block
  - Encapsulating bundle can have simpler primary block than encapsulated bundle.

Proposed Changes

1. Specify a bundle-in-bundle encapsulation (BIBE) protocol
2. Build a “streamlined” BSP which assumes the existence of BIBE.
3. Write a security practices document showing how SBSP+BIBE provides security services equivalent to those provided by BSP.



Streamlined BSP Overview

- Three security blocks, not four
  - Bundle Authentication Block (BAB), Block Confidentiality Block (BCB), Block Integrity Block (BIB)
- Concept of “security operation” as (service, target)
  - (integrity, payload), (confidentiality, payload)
  - Only 1 unique instance of a security operation in a bundle.
- Extension blocks treated same as payloads
  - Extension block no longer replaced by security block.
  - Support for integrity of extension blocks
    - *(integrity, extension_block_1), (integrity, extension_block_2)*
  - Support for primary block integrity
    - *(integrity, primary_block)*
- Goal: minimal change to BSP for simple cases
  - “Simple” cases capture most deployments today.

APL

SBSP: Terminology (1/2)

New terms for security concepts.

- Security-Service
  - Authentication, Confidentiality, Integrity
- Security-Target
  - Block to which a service is applied.
  - Need to uniquely identify every block in a bundle
    - *can't rely on an extension block's order in a bundle*
- Security-Operation
  - *Unique* combination of service/target.
    - *OP(authentication, bundle), OP(confidentiality, primary)*
    - *OP(integrity, extension_block_1), OP(integrity, extension_block_2)*
  - Operation MAY require 1 or more physical blocks.
  - MAY NOT be applied more than once in a bundle.
    - *OP(confidentiality, payload), OP(confidentiality, payload) not allowed*
    - *OP(integrity, block N), OP(integrity, block N) also not allowed.*

APL

SBSP: Terminology (2/2)

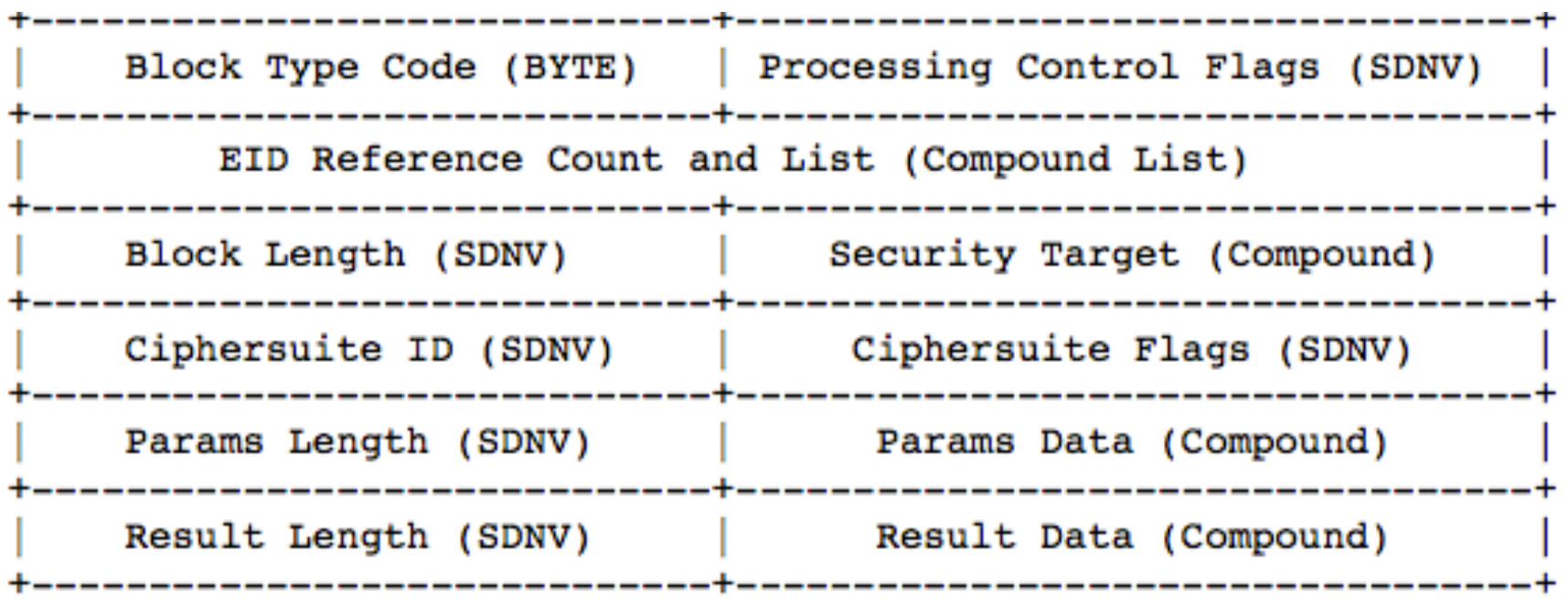
New terms added to differentiate multiple security blocks that comprise a single "security operation".

- Lone Block
  - Used when a single SBSP block is used to implement a single security operation.
    - *Ex: OP(confidentiality, payload) will result in a Lone BCB.*
    - *Ex: OP(authentication, bundle) with a single-block ciphersuite will result in a Lone BAB.*
- First Block / Last Block
  - Used when multiple SBSP blocks implement a single security operation.
    - *Ex: OP(authentication, bundle) with a two-block ciphersuite will result in a "First BAB" before the payload block and a "Last BAB" after the payload block.*
- No terms for blocks between "First" and "Last".
  - No evidence we need > 2 blocks for a security operation.

APL

SBSP – Abstract Security Block

- Correlator field is no long present.
  - Less need for correlation with simplified rules for security operations.
- Security-target new, compound field for block identification
- Security-dest in EID list is optional.
  - For BIB or BCB, destination MUST be bundle destination
  - For BAB, optional and when given, must be the envisioned next hop.



SBSP: Security Target

We need a mechanism for uniquely identifying a block in a bundle.

- No block identification mechanism in RFC5050
  - Note: RFC5050 should provide a block identifier.
- Identify blocks as <blocktype><enumeration>
  - Block type as encoded in the block
  - Enumeration is a simple SDNV count
    - *The Nth instance of the block in the bundle (not based on bundle order)*
    - *NOT required to be monotonically increasing. Gaps OK.*
- Implementation recommendation
  - Create special EID and put it in EID list of blocks in a bundle.
    - *Scheme is the block type*
    - *Scheme-Specific-Part is the enumeration SDNV.*
  - Can be added every time a block is added
  - Can be added on-demand (if not already there) when a SBSP block targets an existing block.

SBSP: Block Types (1/2)

SBSP security blocks treat all security targets the same.

- Bundle Authentication Block (BAB)
  - Authentication over the entire bundle, similar to RFC6257 BAB.
  - Security-target set to 0, always applied to whole bundle.
  - Only block that MAY specify a security-destination.
  - May define multi-result ciphersuite in lieu of multiple BABs
    - *Simplifies protocol support. Moves complexity to ciphersuite handlers where it only affects those needed that ciphersuite.*
- Block Integrity Block (BIB)
  - Similar to RFC6257 PIB, but applies to blocks other than the payload.
    - *Allows primary block as a security target.*
  - Restrictions on security target to prevent “recursion”
    - *A BIB cannot target any other SBSP block type.*
  - May define ciphersuite for multiple security signatures in lieu of multiple BIBs for a given target.

SBSP: Block Types (2/2)

- Block Confidentiality Block (BCB)
  - Similar to RFC 6257 PCB, but applies to blocks other than the payload.
  - May target payload block, any non-SBSP block, and an SBSP BIB.
    - *No support for super-encryption. We recommend super-encryption be handled via encapsulation.*
  - Does NOT fully encapsulate security target.
    - *As with PCB, only data portion of the block is replaced by ciphertext.*
    - *In special cases where other parts of a block require confidentiality, encapsulation or other mechanism may be used.*
    - *BCB may include additional authenticated data to integrity-sign parts of the target block not otherwise covered by the ciphersuite, such as the target-block EID references.*

APL

SBSP: Block Interactions

- A few concerns with BCB/BIB interactions
  - When applying confidentiality to a target, confidentiality MUST be applied to any integrity also applied to the same target.
    - *A BIB won't verify if its target has been encrypted with a BCB after the BIB was created.*
    - *i.e., when adding a BCB for a target, MUST add a BCB covering a BIB for that target, if such a BIB exists.*
  - Integrity processing cannot evaluate an encrypted BIB.
    - *BIB may not be evaluated if it is the security-target of a BCB in the bundle.*
  - Integrity processing cannot evaluate an encrypted security-target.
    - *Security-target contains ciphertext and will not match the BIB integrity signature.*
- SBSP mandates processing order for SBSP blocks
  - BAB evaluated first.
  - All BCBs evaluated before any BIBs.

SBSP: Canonicalization and Fragmentation

- Changes to canonicalization
  - Bundle Canonicalization
    - *Largely same as RFC6257, including nits, errata*
  - Primary-Block Canonicalization
    - *To allow for primary block integrity.*
  - Payload-Block Canonicalization
  - Extension-Block Canonicalization
- Fragmentation
  - Integrity and confidentiality MAY NOT be applied to a fragment.
    - *Even if security-target is not the payload.*
    - *May use encapsulation if this feature is required in a network.*
  - May NOT fragment a bundle with a BAB.
    - *Fragmentation must occur before calculating authentication information.*
    - *BABs may be added to fragments.*

APL

SBSP: Bundle Example (1/2)

Example of common security features in a single bundle

- Bundle
  - Primary block, payload block, and two extension blocks
- Authentication
  - Add BAB to the bundle using a two-BAB ciphersuite
- Integrity
  - Sign the primary block
  - Sign the second extension block
  - Sign the payload
- Confidentiality
  - Encrypt the first extension block.
  - Encrypt the payload block
    - *By SBSP rules, encrypt the BIB providing integrity to the payload block as well.*

APL

SBSP: Bundle Example (2/2)

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