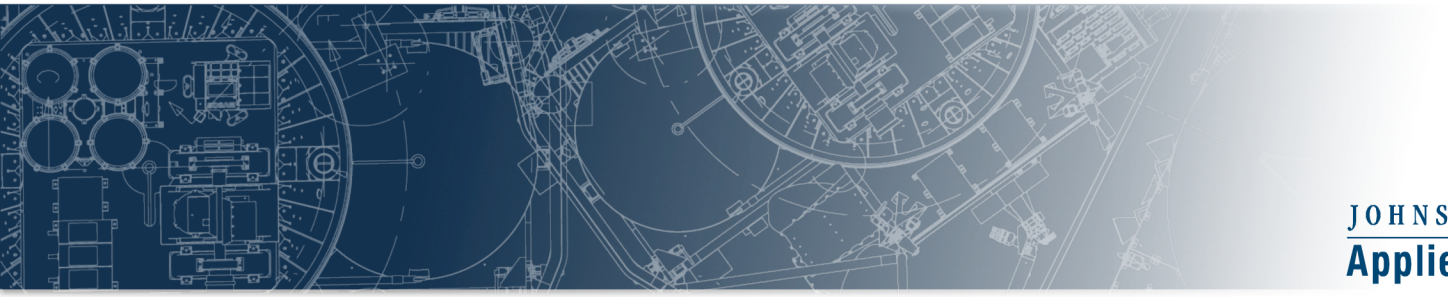
BPSEC Updates

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



JOHNS HOPKINS UNIVERSITY
Applied Physics Laboratory

UART Slide

- Updates
  - Updated introduction, general cleanup, sync to BPBis
- Additions
  - Added multi-target capability to security blocks
  - Added encoding for canonical forms
  - Added security considerations section
  - Added ciphersuite authorship considerations section
- Removals
  - Removed concept of First/Last Block
  - Removed all CMS Block related content.
  - Whole-block canonicalization
- TODO
  - Open questions
  - Next steps

Updates to Sections 1/2

- Section 1: Introduction
  - General editorial clean-up of the text in the Intro section.
    - *Reworded Motivation section*
    - *Minor rewording elsewhere*
    - *Removed text graphic of bundle nodes – duplicate from BPbis. Not seen as very helpful.*
    - *Consolidated terminology section.*

- Section 2: Key Properties
  - General editorial clean-up of the Key Properties Section

Updates to Section 3 (1/2)

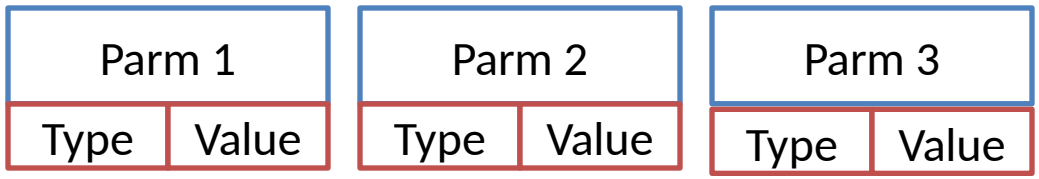
- Added a few new sections to centralize technical concepts. No technical change from previous documents.
  - Added “Uniqueness” section to discuss uniqueness of security operations in a bundle.
  - Added “Target Multiplicity” section to discuss how to target multiple blocks at once, and necessary conditions.
  - Added “Target Identification” section to discuss usef of Bpbis Block Number to represent security targets.,
- Updated section to track Bpbis
  - Block fields for CRC type and CRC value
  - Updated Abstract Security Block structure to align with Bpbis and CBOR encoding.

Updates to Section 3 (1/2)

- Updated Abstract Security Block description
  - Added CBOR encodings for abstract security block
  - Changed flag bit description to match Bpbis
    - *No change to bits themselves.*
- Minor changes to BIB and BCB sections
  - Point to tables for block Id instead of hard-coding.
  - Cleaned up order of some information.
- Parameters and Result Types
  - Gave Parameters and Results different enumeration spaces
  - For each such space, gave a CBOR encoding for the values.
  - Added reserved and unassigned sections for each.

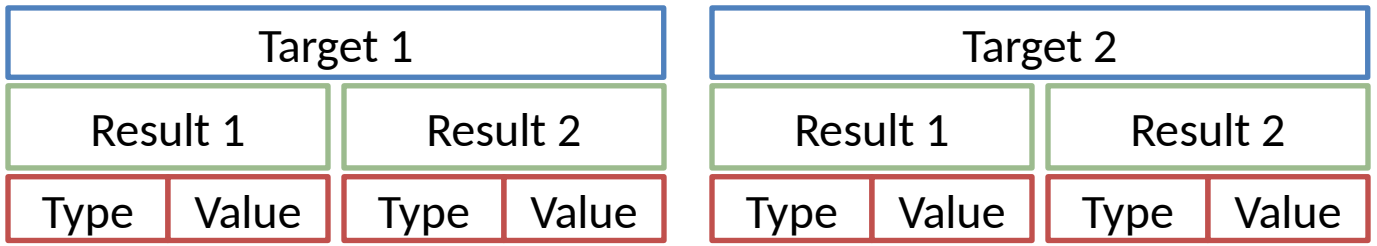
CBOR Encodings (1/2)

- CBOR Types
  - Security targets: CBOR array of unsigned integers
  - Cipher Suite Id: CBOR unsigned integer
  - Cipher Suite Flags: CBOR unsigned integer
  - (opt) Security Source: CBOR array in accordance with Bpbis rules for EID representation.
  - (opt) Cipher Suite Parameters: CBOR array of parameters
    - *Each parameter is a CBOR array of type/value.*
    - *Type is a CBOR unsigned integer enumerating type of parm.*
    - *Value is encoded as the CBOR type for the parameter.*



CBOR Encodings (2/2)

- CBOR Types
  - Security Result: CBOR array of targets
    - *Each target is a CBOR array of results.*
    - *Each result is a CBOR array of type/value.*
    - *Type is encoded as a CBOR unsigned integer*
    - *Value is encoded as the CBOR encoding of the result type.*



Parameter Types

Type	Name	Description	CBOR Encoding
0	Initialization Vector	A random value, typically eight to sixteen bytes.	Byte String
1	Key Information	Material encoded or protected by the key management system and used to transport an ephemeral key protected by a long-term key.	Byte String
2	Content Range	Pair of unsigned integers (offset,length) specifying the range of payload bytes to which an operation applies. The offset MUST be the offset within the original bundle, even if the current bundle is a fragment.	CBOR array comprising a 2-tuple of CBOR unsigned integers.
3	Salt	An IV-like value used by certain confidentiality suites.	Byte Array
4-31	Reserved	Reserved for future BPSec protocol expansion	
>= 32	Unassigned	Unassigned by this specification. Can be assigned by cipher suite specifications.	

Result Types

Type	Name	Description	CBOR Encoding
0	Integrity Signatures	Result of BIB digest or other signing operation.	Byte String
1	BCB Integrity Check Value (ICV) / Authentication Tag	Output from certain confidentiality cipher suite operations to be used at the destination to verify that the protected data has not been modified. This value MAY contain padding if required by the cipher suite.	Byte String
2-31	Reserved	Reserved for future BPSec protocol expansion	
>= 32	Unassigned	Unassigned by this specification. Can be assigned by cipher suite specifications.	

Updates to Section 4: Canonical Forms

- Primary Block Canonicalization
  - Updated to Bpbis format and Bpbis CBOR encoding
  - Mask out “bundle if fragment” and “custody transfer requested for this bundle”
  - Reserved bits in flags to be represented as 0 for canonicalization.
- Non-Primary Block Canonicalization
  - Follows bpBis block canonicalization rules with exceptions
    - *Confidentiality operations omit block type code, block number, block processing control flags, CRC type, and CRC field and block data length fields (e.g., the block header).*
    - *May apply to a subset of the block data based on content range.*

Updates to Other Sections

- Minor grammar/editorial updates
  - Section 5: Security Processing
  - Section 6: Key Management
  - Section 7: Policy Considerations
  - Section 8: Security Considerations
  - Section 10: Other Security Blocks
  - Section 11: Conformance
- Section 9: Cipher Suite Authorship Considerations
  - Added that new BPSec cipher suites should consider adding new cipher suite parameters, result types, and canonicalization algorithms if necessary.
- Section 12:
  - Cleaned up IANA considerations section.
  - Will need help here.

Thank you!

Questions?