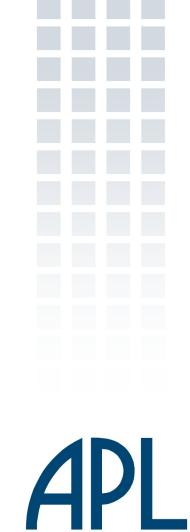
BPSEC Updates

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





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 Intro Section

- Added Motivation Section
- Added Section to Define/List Supported Services
 - Confidentiality, Integrity and rationale for no authentication:
 - 1. Term Hop-by-Hop ambiguous in an overlay
 - 2. Not every node security aware
 - 3. Hop-by-hop authentication special case of integrity
- Added Scope Section
 - BPSEC does not address
 - Ciphersuite implementations, Security Policy
 - Combination of this spec and others to achieve specific outcomes
- Params and Results section
 - Specified which items are for which field.
- Updated security blocks example
- Cleaned up fragmentation section.







Addition: Multi-target Blocks

- At earlier IETF decided not to have 1 BPSEC block per service.
 - Instead, each block would have a unque identifier and could be targeted by a BCB or a BIB. With multiple BCBs and BIBs in a bundle.
- Optimization: IFF a set of security targets share security source and key information, represent them with 1 security block.
 - Security block will have a list of security targets and a list of security results.
 - Avoids redundant capture of key configuration and extra block processing.
 - Still allows different key configurations and different security sources to manage their own blocks.







Addition: Canonical Encoding

- Updated canonical forms section
 - Synchronized block canonical forms with updates to BPBis.
 - Dropped dictionary, added CRC flag and content, changes to flags that need to be omitted from a canonical form, etc...
- Provides encoding for each block
 - BPBis does not provide an encoding.
 - What happens if a security source uses a different encoding than a someone than the bundle destination or security-aware waypoint?
 - If BPSEC does not provide an encoding, do we force encoding gateways to also be security gateways?
 - Encoding likely to be updated to CBOR.







Addition: Security Considerations

A security review of BPSEC performed

- Separate from ciphersuite review, policy review, or bestpractices-of-implementation review.
- Looking for weaknesses in the extension-block approach of BPSec itself.

Major findings

- BIB and BCB blocks provide good protection, but you need to know when to expect them.
- Ciphersuites populating security blocks are responsible for defense against replay (nonce, chaining, etc...)
- Some out-of-band mechanism (policy) need to let nodes know when to expect what security blocks.
- BIBs must be encrypted with a BCB when leaving a secure enclave to avoid re-signing.





Addition: Ciphersuite authorship considerations

- Security review identified some areas where cipher suites must fill in gaps for BPSec.
- Capture these items in a section in this spec.
 - No major changes, but things to consider as a function of
 - Data Lifetime
 - Possibility of one-way traffic
 - Opportunistic and session-less operation.
 - For example, BPSec by itself has no mechanism for preventing replay of BCBs or BIBs. Nor should it, as this can be handled in the ciphersuite layer.





Removed

- First/Last block concept
 - Removed all language referencing first/last block
 - Removed ciphersuite flags relating to whether results were present in a block or not
 - With only 1 block per security operation, it has to have a security result in it.
- CMS Block
 - Removed text describing block and updated block interactions section.
- Whole-bundle canonicalization
 - Without an authentication block, no need for a whole-bundle canonicalization.
 - Other specs can identify such a block if they wish, and then that block can be protected by a BIB.





TODO

Planned changes:

- No more major planned changes. Some items identified already:
 - MUST used instead of must in 2 places
 - Section 3.7 needs to identify minimum parameter set and change wording to not apply to fragments.
 - Remove Section 10 "Conformance"
- Will likely review encoding and security/policy considerations sections as we process feedback.

Open Questions

- Should BPSec provide an encoding?
- If yes, should the encoding be optional or mandatory?
- Does BPSec really need blocks transmitted in order?





BPSEC ADM

- Queryable Data (54 items)
 - Successful/Unsuccessful TX/RX of BCB/BIB by # blocks and # bytes.
 - Missing-on-RX and Forwarded of BCB/BIB by # blocks and # bytes
 - Statistics reportable by both "totals" and for a given EID.
 - Also reports metrics for "anonymous" bundles.
 - Known key names, ciphersuites, and policy rules
- Reports: (2 items)
 - Report on all metrics summed for all EIDs
 - Report for metrics for a given EID.
- Controls (9 items)
 - Reset Counts (total, or for a given EID)
 - Key: Add/Remove key
 - Rules: Add, Update, Delete, List BCB and BIB rules
 - Rule: {SRC, DST, Security-Target, Ciphersuite, Key}







What next?

- Currently have 3 expired drafts that need to be considered
 - Security Best Practices
 - <u>https://tools.ietf.org/html/draft-birrane-dtn-sec-practices-00</u>
 - Expired July 1st, 2016
 - Suite-B Profile for BPSec
 - <u>https://tools.ietf.org/html/draft-birrane-dtn-bpsec-suiteb-profile-00</u>
 - Expired July 3rd, 2016
 - Suite-B Ciphersuites for BPSec
 - https://tools.ietf.org/html/draft-birrane-dtn-bpsec-suiteb-ciphersuites-00
 - Expired July 3rd, 2016
- Should any of these also be considered by the WG?
 - Much like BPBis, do we need a ciphersuite identification/profile for BPSec to take BPSec to last call?







Questions?



