BPSEC Updates

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

- Removed Authentication Blocks
- Removed Security Destinations
- Removed Bundle Canonicalization
- Simplified Block Identification
- Updated Security Block Formats to BpBis-03
Authentication is a special case of integrity and does not need its own dedicated block.
- We need authentication.
- We do not need a dedicated BAB block to achieve it.

Five ways proposed to get (levels) of authentication
- Use trusted convergence layers instead
- Sign a block representing previous hop (PHN) with a BIB
- Sign several (every) block with several BIBs
- *Define a multi-target BIB and sign several/every block with that.
- Define a bundle-wide hash block and sign that with a BIB

*Only 1 of the above options would require a change to BPSEC (covered later)
Removed Security Destinations

- Removed security destinations from BPSEC blocks.

- BPSEC-aware BPAs evaluate BPSEC blocks as a matter of their local policy.
  - Such BPAs will determine if they should verify a BIB
  - Such BPAs will determine if they should decrypt a BCB target.
  - Having a security destination either:
    - Couples security and routing
    - Forces security processing at the bundle destination

- Security Sources Remain
  - Optional ability to state who initiated a security operation.
  - Can have different security sources for different blocks.
**Other Updates**

- **Whole-bundle canonicalization necessary for BAB blocks**
  - Generate an immutable version of the serialized bundle useful for hashing.
  - Still a viable method for doing hop-by-hop authentication of an entire bundle, but should not be part of BPSEC.

- **Simplified Block Identification**
  - BPSEC block targets can now be specified using the block identifier rather than inserting a contrived EID reference.

- **Updating BPSEC to track changes in BPBIS.**
  - Changing BPSEC block headers to match BPBIS.
  - Need to change block canonicalization algorithms to match BPBIS.
Planned Changes

- Expanded and revised security section to include:
  - Analysis of BPSEC CONOP resilience to common attack vectors (for example: man in the middle – inserting, deleting, modifying blocks).
  - Recommendations for Cipher Suite Developers
  - Recommendations for Policy Developers

- Expand Desirable Properties Section
  - Add Assumption and Constraints

- Some open questions remain
Open Questions (1/2)

- Can we remove First/Last Block concept?
  - BAB had supported one pre-payload and one post-payload.
  - BPBIS may have payload be the last block in a bundle.

- Should the BIB and BCB content itself be signed?
  - Security source, ciphersuite parameters, etc…

- Do we want to keep the CMS Block?
Open Questions (2/2)

- Should we allow a BIB and BCB to have multiple targets?
  - Different than block multiplicity. Still need multiple BIBs/BCBs:
    - With different security sources, different ciphersuite selections, different parameters.
  - Can optimize IFF security services have all config in common:
    - Same security source
    - Same ciphersuite and ciperhsuite parameters
  - Multi-target block would have N targets and N security results. Share common security source and other parameters.
  - PRO: One BIB or BCB could be used instead of N BIBs or BCBs
    - Less duplication of data (block types, sizes, ciphersuite parms)
    - Big space savings when using asymmetric key encryption
  - CON: How do we remove targets from a multi-target BIB/BCB?
    - Some surgery on blocks by someone other than security source.
Thank you!

Questions?