BPSEC Updates

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

- Summary
- Updates
- Outstanding Comments
- Interoperability Cipher Suites
- Next Steps
Motivation for this document

- In-bundle security mechanism is needed in some cases
  - Different blocks may have different security needs
  - Different nodes may impose different security policy
- If you do not want in-bundle security, you can secure BP by having
  - Users protect their data at the application layer (e.g. secure payload)
  - Users select secure convergence layers (if they exist)

Design decisions

- Different blocks in a bundle can have different security
- Processing order must be unambiguous at a receiver
- New cipher suites must be able to be added at future dates
Summary (2/3)

- **Block Format**
  - Two new extensions blocks defined
    - Both capture list of targets they act upon, key information, cipher suite configuration, and result information.
    - Integrity (BIB) – Holds signature
    - Confidentiality (BCB) – Indicates target(s) have had their block data replaced with crypto-text
  - A security block can target 1 or more other blocks
    - Multiple targets prevents redundant info in the bundle.
  - Mechanism provided to add new security blocks in other documents if necessary.

- **Block Processing Rules to Enforce Determinism**
  - If a BCB target is encrypted, a BIB on that target is also encrypted.
  - A BIB cannot target a BCB or a block protected by a BCB.
    - There exist BCB cipher suites that also generate integrity signatures
  - At a receiver, BCBs must be processed before BIBs.
Block Processing (cont)
- Cannot add BIBs and BCBs if bundle represents a fragment.
  - Can encapsulate in that case.
- Nodes determine if they are a security destination by policy.
  - Dangerous and confusing to have bundle assert internal to itself what the security destination would be.

Security Considerations
- Brief review of attacker types in a DTN, explaining how to apply BCB and BIB in these cases.
- Explanation for why security policy should be out-of-band configured in the network and not included in the bundle itself.
  - Namely, a bundle might have blocks dropped by a malicious BPA, so blocks that encode security requirements cannot be relied on.
Updates to Sections 1/3

- **General**
  - Minor editorial clean-up through all sections

- **Section 3.5: Block Representation**
  - No duplicate targets allowed in a target list.
  - Cipher Suite Parameters: Added illustration. Ref. section 3.10
  - Security Results: Added illustration. Ref section 3.10
Updates to Sections 2/3

Section 3.10 – Cipher suite Parms and Result IDs

- Removed tables of parameter and result types.
- Noted that these have value within the context of individual cipher suites.

“Cipher suite parameters and security results each represent multiple distinct pieces of information in a security block. Each piece of information is assigned an identifier and a CBOR encoding. Identifiers MUST be unique for a given cipher suite but do not need to be unique across all cipher suites. Therefore, parameter ids and security result ids are specified in the context of a cipher suite definition.”

A cipher suite MAY include multiple instances of the same identifier for a parameter or result in a security block. Parameters and results are represented using CBOR, and any identification of a new parameter or result MUST include how the value will be represented using the CBOR specification. Ids themselves are always represented as a CBOR unsigned integer.
Updates to Sections 3/3

- **Section 4 – Canonical Forms**
  - Removed custom canonicalizations of the primary block.
  - All non-primary blocks canonicalized as in BPBis, with following exceptions:
    - *When canonicalizing for confidentiality only include the block type specific data.*
    - *Reserved flags, when specified, are never included in the canonicalization.*

- **Removed conformance section (Section 11 in -04)**

- **Section 11 – IANA Considerations**
  - Identified need for registry of cipher suite identifiers.
  - Allocated table for BIB and BCB block types (currently TBD)

- **Section 13 – References**
  - Added COSE as an informative ref.
Some comments received after publish of -05.

Request that comments go to the mailing list.

Summary:

- Allow cipher suites to specify how cipher suite parameters and results are stored within the security block, instead of specifying it in section 3.10.
  - Essentially make that part of the security block “opaque” and determined by the cipher suite selected.

- Five cases where MUST is being over-used.

- Section 8.2.2 makes assertions about the security of sign+encrypt which are too strong
  - (e.g. that an attacker cannot successfully modify a bundle if they cannot decrypt the bundle).
  - Instead, in this situation require a IND-CCA2 encryption scheme.
Interoperability Cipher Suites

- Published draft of BPSec interoperability cipher suites
- Integrity
  - BIB-HMAC256-SHA256
    - The integrity cipher suite provides a signed hash over the security target based on the use of the SHA-256 message digest algorithm [RFC4634] combined with HMAC [RFC2104] with a 256 bit truncation length. This formulation is based on the HMAC 256/256 algorithm defined in [COSE] Table 7: HMAC Algorithm Values.
- Confidentiality
  - BCB-AES-GCM-128
    - The confidentiality cipher suite provides cipher text to replace the data contents of the target block using the AES cipher operating in GCM mode [AES-GCM]. This formulation is based on the A128GCM algorithm defined in [COSE] Table 9: Algorithm Value for AES-GCM.
Next Steps

- **BPSEC**
  - No significant problems with BPSec have been identified.
    - Section -04 to -05 addressed minor updates resulting in not over-specifying in the draft.
    - Largest remaining issue appears to be whether BPSec requires formatting of cipher suite specified configuration parameters and results.
  - Can we resolve this minor issues in the context of last call?

- **Interoperability Cipher Suites**
  - Need a short period of review and updates.
  - Likely ready for a last call at next IETF.
Questions?