BPSSec Updates

IETF-106

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

- BPSec v12 Review Comments
- BPSec v13 Updates
- Remaining BPSec Activities
- Interoperability Cipher Suites
  - Single-Target, Multi-Result
- Security Context Policy Rules
bpsec-12 reviews

1. GenArt
   - Ready with nits
   - Under section 1.4, BPA is referenced in bullet 1 and 2 but is first defined in bullet 4. Suggest defining that in bullet 1.
   - "never used to sign the cipher-text provided" has an extra space between cipher- and text.
   - "The BCB is decrypted by security-aware nodes in the" has an extra space between security- and aware.

2. Sec-AD
   - Pending
1. **IANA**
   - Converged on the registry questions in the new Bundle Protocol specification, agreeing to register new BPv7 block type numbers in the existing Bundle Block Types registry rather than starting up a new registry for BPv7 block types.
   - Block type numbers 2 and 3 -- originally requested for the BPsec BIB and BCB blocks -- are not available (they are used by the old Bundle Authentication Block and Payload Integrity Block), so we must assign from one of the unassigned ranges.
   - The BPbis specification requests that block types 11 and 12 be reserved for the Block Integrity Block and Block Confidentiality Block respectively, so those are the values that I would propose we assign.
   - A slightly revised BPsec Internet Draft will be posted that simply requests that IANA assign numbers for these two blocks, without specifically asking for any particular values, so in the end I think there will be no conflict.
bpsec-13 updates

1. Minor changes
   - No technical change to the standard, data structures, or processing.

2. Corrected Gen-Art nits.

3. Clean up some terminology
   - Bpsec-12 had some remaining references directly to key parameters instead of the more general security context parameters.
   - Ensured consistent use of security context terminology versus cipher suite terminology.
   - Fixed description error in the BPSec example.
   - Changed BIB and BCB block types to 11 and 12
     - May need to change to “IANA assigned” and not hard-code to 11/12
Remaining bpsec activities?

- Waiting for security ad reviews
  - Initial review from bpsec-06. Comments from that review have been incorporated.

- Updated IANA section
  - Final edit to ensure that the IANA section is correct regarding block types.

- Terminology updates
  - The use of term “EID-reference” should be updated to just say “EID” to avoid confusion with the BPv6 concept of bundle dictionaries and EID references into dictionaries.

- Any other review comments.
Variety of security context concepts

- **Self-signing BIB**
  - Store an integrity signature on the target block.
  - Store an integrity signature on the BIB itself (parameters, targets)

- **Single-Target, Multi-Result BIB**
  - Hold multiple security results per target.
  - Security context defines potential for multiple key parameters

- **Questions for interoperability security context**
  - BIB: Should the signature be calculated over the entire target block (including extension block header) or simply over the block type-specific data fields?
  - BCB: Should BCB calculate separate plain-text signature over extension block header?
What are policy rules?
- Out-of-band configurations for how to apply/process security blocks.
- Must be separate from information in a bundle.
  - Bundle contents can be manipulated by a malicious actor, so bundles must not solely encode security policy.
  - Example: An actor removes a BIB, then changes a BIB target. A receiver must know that a BIB is required to detect this malicious change.

Roles and Responsibilities
- Security Source
  - Responsible for determining which security services should be added to a bundle.
  - May or may not be the bundle destination.
- Security Waypoint
  - Responsible for (optionally) verifying security services.
- Security Destination
  - Responsible for processing and removing security services.
  - May or may not be the bundle destination.
Bpsec policy roles
What is a source rule?

- A definition which can be matched against a bundle
- If block matches some criteria, then apply given security service.

Requires 6 pieces of information

1. Bundle Source (EID)
2. Bundle Destination (EID)
3. Target Block Type
4. Security Source (EID)
5. Security Context ID
6. Security Parameters

Example

- {"ipn1.*", "*", 1, "ipn1.0", 7, "keyname=1"}
- Any payload block originating from IPN node 1 going anywhere should be integrity signed using security context ID 7 with the given parameters
What is a waypoint/destination rule?
- A definition which can be matched against a bundle
- If block matches some criteria, then apply given security service.

Requires 6 pieces of information
1. Bundle Source (EID)
2. Bundle Destination (EID)
3. Target Block Type
4. Expected Security Context ID
5. Asserted Local Security Parameters
6. Processing Actions

Example
- `{“ipn1.*”, “*”, 1, 7, “keyname=1”, 0xAA}`
- Any payload block from IPN node 1 must have a security source for context ID 7, verified with local parameters. On success or failure, perform following actions.
A bitfield to describe potential actions when processing a security service.

- Bit 0 (the low-order bit, 0x01): Follow the block processing control flags of the security target which failed during processing.
- Bit 1 (0x02): Follow the block processing control flags of the security block corresponding to the security target which failed during processing.
- Bit 2 (0x04): Send report to bundle's report-to EID.
- Bit 3 (0x08): Delete the security target that failed during processing.
- Bit 4 (0x10): Delete the security block associated with the security target that failed during processing and all of its security targets.
- Bit 5 (0x20): Delete bundle.
- Etc…
Bpsec policy roles – example