BPSec:
AD Review Comments and Responses

Ed Birrane

Edward.Birrane@jhuapl.edu

Overview

- 11 comments received.
- Result: 6 proposed changes to the document
  1. Reference security context document.
  2. Define term “security processing node”.
  3. Clean up security processing flags
  4. Clarify what is meant by consolidating signatures in multi-block BIBs.
  5. Remove guidance on selecting context IDs
  6. Add section on context registry in the IANA considerations.
- Propose no changes to the processing or structure of the specification
- Happy to clarify or add other text as needed.
- Walk through comments in following slides.

1. Reference Security Context Document

- Section 1.2 (Specification Scope)

❑ As the WG actually have one example specification for a security context and cipher suits, it would be good to reference this so that people realize that it exist and can be looked at in parallel.

✓ Agreed. A reference to the security context document will be added to Section 1.2

2. Add Term for Peer Source

- Section 1.4 (Terminology)

❑I am missing a term for the receiver / target either if that is any holder of the security context or an intended bundle receiver, in other words the peer to security source.

✓Originally removed the concept of “security destination” from the specification as it conflated security processing and bundle routing. We can add a term for “security processing node” as the general BPA which may process a security block, but that processing node is not necessarily known in advance and not guaranteed to be the bundle destination.

3. BIB over BCB? (1/2)

- Section 3.1 (Block Definitions)

- This is only part of a conflict between the order between BIB and BCB processing and the possibility for a node along the Bundle path to verify the integrity of parts of the bundle. So my thoughts here is that bundle sender has two security contexts. One with the receiver that it will use to secure the BUNDLE Payload and other Blocks that are of end-to-end nature and not needed on path. Then I will have another security context that a set of the bundle forwarding nodes share so that they can verify the bundle being sent. However, to my understanding this is not possible as any BIB using the second context can't use encrypted payload block as its input. So although the documents talks about this, it appears to have limited utility. Any comments about this limited utility?

3. BIB over BCB? (2/2)

- ✓Need to avoid circular dependency of BIB and BCB. BIB is used for signing plaintext only. BCB is used to generate AND sign ciphertext.

- ✓This is captured in Section 7:
- ✓Adding a BIB to a security target that has already been encrypted by a BCB is not allowed. If this condition is likely to be encountered, there are (at least) three possible policies that could handle this situation.
  - ✓At the time of encryption, a plain-text integrity signature may be generated and added to the BCB for the security target as additional information in the security result field.
  - ✓The encrypted block may be replicated as a new block and integrity signed.
  - ✓An encapsulation scheme may be applied to encapsulate the security target (or the entire bundle) such that the encapsulating structure is, itself, no longer the security

4. Context Part of Uniqueness?

- Section 3.2 (Uniqueness)

❑This uniqueness requirement, isn't this missing a dependency on security context? To me there appear that being able to use more than one security context has some benefits, or is it making things to complex, or are there other reasons?

✓Discussed in the WG. Makes things very complex: how to handle a block that decrypts with some keys but not others. Same with authentication. BPSec does not prevent multi-key (or even multi-algorithm) encryption, but the approach is to handle this by defining a security context for this work, and not to build it piece-by-piece in a network by adding new BCBs to the bundle.

5. Reserved Bits

- Section 3.6 (Abstract Security Block)

❑Security Context Flags: What is the meaning of the Reserved bits? What should the sender and receiver do with these bits. Can they be assigned in the future?

✓Reserved bits selected to help backwards compatibility with reference implementations. Bits 4 and 5 can be migrated to bits 2 and 3 and have this be a 3 bit field. Recommend making this a byte field with 8 bits of flags and instruction that reserved bits be ignored by implementations.

6. Why require AEAD cipher suite?

- Section 3.8 (Block Confidentiality Block)

❑The Security Context Id MUST utilize a confidentiality cipher that provides authenticated encryption with associated data (AEAD). Why is AEAD a requirement? If the requirement is that no confidentiality without integrity, then that can be stated in an other way than requiring AEAD.

✓Early sec review comments stated that AEAD was a requirement.

7. Policy Guidance for stripped blocks (1/2)

- Section 3 (Security Blocks)

- ❑ Looking at the BIB and how it is structured and how the signature is created and stored with one signature per block implies that any on path attacker can remove individual blocks without it being noticed. So aren't there a missing possibility to create a BIB that actually ensures that if it validates a set of blocks was correctly provided? I know that with the current mechanisms such a BIB could be stripped. However, such a block could easily be required in a security policy for a particular deployment. Was such aspects considered?

7. Policy Guidance for stripped blocks (2/2)

- ✓Future extension blocks, such as a signed manifest block, proposed. You require the manifest block and the manifest block identifies other needed blocks. But any particular policy outside of the scope of BPSec document.

- ✓Section 8.2.2: Since BPSec security operations are implemented by placing blocks in a bundle, there is no in-band mechanism for detecting or correcting certain cases where Mallory removes blocks from a bundle. … In each of these cases, the implementation of BPSec must be combined with policy configuration at endpoints in the network which describe the expected and required security operations that must be applied on transmission and are expected to be present on receipt. This or other similar out-of-band information is required to correct for removal of security information in the bundle.

8. Clarify Section 3.9 on consolidating BIBs

- Section 3.9 (Block Interactions)

❑This comment is linked to the pervious one. When reading this, I had a hard time to understand what “moved” in the above text actually meant. Finally I realized that you could actually move a signature from one BIB to another. I think this could be made a bit clearer.

✓We can clarify this text to say move a signature from one BIB to another.

9. Part of Section 3.10 unclear

- Section 3.10 (Parameter and Result Identification)

❑ ”*Individual BPSec security context identifiers SHOULD use existing registries of identifiers and CBOR encodings, such as those defined in [RFC8152], whenever possible. Contexts SHOULD define their own identifiers and CBOR encodings when necessary.*”

  - I find the above paragraph unclear. I think one part is what “security context identifiers”.

✓This text was added to satisfy a comment from Stephen Farrell noting that there exist cipher suite identifiers for some cipher suites and it would be confusing to make new enumerations for BPSec. Since BPSec now uses security contexts, these comments no longer useful.

10. How is a Security Destination Determined?

- Section 5.1.1 (Receiving BCBs)

❑*"If the receiving node is not the destination of the bundle, the node MUST decrypt the BCB if directed to do so as a matter of security policy."*
  - I think this is an example of the unclarity of who is to process a particular security block, because I don't understand how the node will be able to do this.

✓The protocol explicitly removed a concept of "security destination" because this conflates routing and security – what if the bundle gets to the bundle destination prior to the security destination? Because bundles are long lived, what if topology changes alter the identification of the decrypting node after the bundle was originally created?

✓BPSec mentions in sections 2.3, 2.5, and other sections that security block processing is part of a security policy that is determined by the bundle receiver, and not the bundle sender.

11. Registry Required

- Section 11 (IANA Considerations)

❑If you need a registry for security context identifiers then you need to create it and defines its rules.

✓Agreed. Will add.