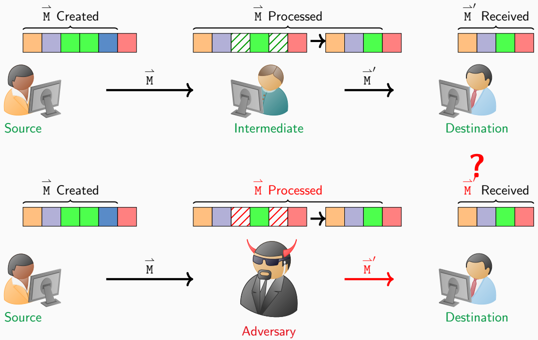
Secure Bundle Audit Mechanism

Bhagya Wimalasiri bhagya.wimalasiri@kcl.ac.uk
Benjamin Dowling benjamin.dowling@kcl.ac.uk
Britta Hale britta.hale@nps.edu
Xisen Tian xisen.tian1@nps.edu

March 13, 2026

SBAM Quick Recap

- Currently dst cannot tell if src-added security ops have been maliciously removed or not.
- SBAM provides end-to-end cryptographic integrity for src-added BPSec security ops between the src and payload dst.
- Preserves standard BPSec behavior, maintains a verifiable record of src-added security ops, even after associated security block is removed.



SBAM Functionality

Add two additional layers of integrity:

Reporting by intermediaries when processing origin security blocks

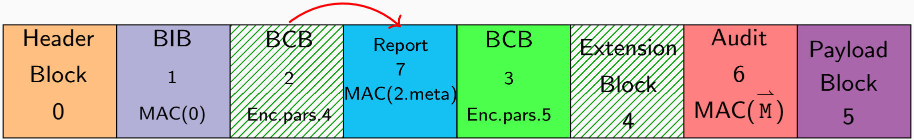
AND

Audit over BPSec params and key info created by bundle src and verified by payload dst

Dst rejects the bundle on audit/report verification failure or audit–report data mismatch.

Guarantees dst one of the following:

1. All security blocks added by the source have arrived unchanged or
2. Some honest intermediate has correctly processed and discarded security block/s



Request for Feedback: New Logical Block ‘audit-pair‘

- **Design**: Manifest + BIB.
  - Manifest records identifiable data for ALL src security blocks.
  - BIB authenticates manifest.
- **Auditing**: Created and verified once per bundle
  - Bundle src creates audit-pair at origin, immutable and mandatory
  - Verified only by dst

```
$$ metadata-item //=(
0  (int16) security-sourcing/security-acceptor
2  embed-eid-structure
3  dtn-time)
$$ blockdata-item //=(
1  block-id - security block#
2  block-control-flags
5  btsd-len
6  [+btsd-hash]
-1 bpsec-targets
-2 bpsec-security-context
-3 key-id)
```

Manifest Block

```
1 security context id:  BIB
2 control-flags
3 block#: block id
4 security context info : algorithms/params/key-id
5 target blocks:  manifest block id
6 security results:  MAC over manifest
7 id.security.src
```

BIB Security Block

Bundle Protocol (BP) Manifest Block (datatracker.ietf.org/doc/html/draft-sipos-dtn-manifest-block-00)

Request for Feedback: New Logical Block ‘report-pair‘

- **Design**: Manifest + BIB
  - Manifest duplicates identifiable data for EVERY src security block processed.
  - BIB authenticates manifest.
- **Reporting**: On demand creation by intermediary, verified once.
  - Created per each discarded src security op
  - Immutable once created
  - Optional, i.e., src security ops may reach dst unchanged
  - Verified only by dst

```
$$  metadata-item //=(
0   (int16) security-sourcing/security-acceptor
2   embed-eid-structure
3   dtn-time)
$$  blockdata-item //=(
1   block-id - security block#
2   block-control-flags
5   btsd-len
6   [+btsd-hash]
-1  bpsec-targets
-2  bpsec-security-context
-3  key-id)
```

Manifest Block

```
1   security context id:  BIB
2   control-flags
3   block#: block id
4   security context info : algorithms/params/key-id
5   target blocks:  manifest block id
6   security results:  MAC over manifest
7   id.security.src
```

BIB Security Block

Request for Feedback: Unique Key Identifiers

- **Requirement**: SBAM designs reciprocal trust dynamic between src, honest intermediary, and dst using unique key identifiers. Within BPSec local security policies *define* keys to use for security context.
- **Problem**: If not standardized, colliding key identifiers may impact protocol correctness; participating nodes may misinterpret keys.
- **Proposal**: `key-id` as an explicit security context parameter (byte string), enabling BPAs to uniquely identify correct keys per context.

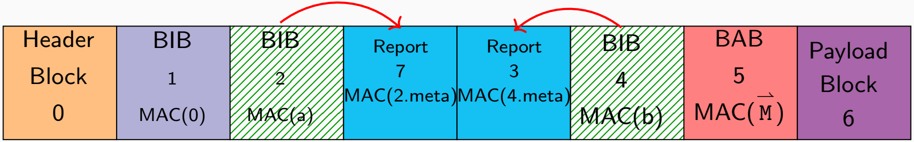
```
$$ metadata-item //=(
0  (int16) security-sourcing/security-acceptor
2  embed-eid-structure
3  dtn-time)
$$ blockdata-item //=(
1  block-id - security block#
2  block-control-flags
5  btsd-len
6  [+btsd-hash]
-1 bpsec-targets
-2 bpsec-security-context
-3 key-id)
```

Manifest Block

```
1 security context id:  BIB
2 control-flags
3 block#: block id
4 security context info : algorithms/params/key-id
5 target blocks:  manifest block id
6 security results:  MAC over manifest
7 id.security.src
```

BIB Security Block

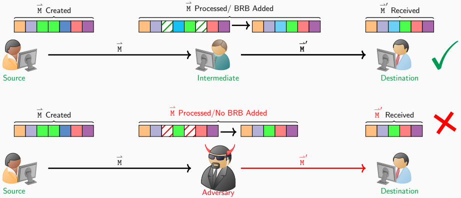
Request for Feedback: Possible Efficiency Extension?



- **Problem:** SBAM introduces overhead: Need to replace BIB/BCB with 'report-pair' (manifest+BIB). Is this ok?
- **Alternative:** Use a single *special* append-only manifest block that contains a MAC authentication field in its block-data map. Replicates the behavior of report-pair without the overhead. BIB over manifest is replaced by MAC over block-data-items.

Summary

- Updated SBAM with Manifest Integration
- `https://www.ietf.org/archive/id/draft-tian-dtn-sbam-03.txt`




```
$$  metadata-item //=(
 0  (int16) security-sourcing/security-acceptor
 2  embed-eid-structure
 3  dtn-time)
$$  blockdata-item //=(
 1  block-id - security block#
 2  block-control-flags
 5  btsd-len
 6  [+btsd-hash]
-1  bpsec-targets
-2  bpsec-security-context
-3  key-id)
```

Manifest Block

```
1  security context id:  BIB
2  control-flags
3  block#: block id
4  security context info : algorithms/params/key-id
5  target blocks:  manifest block id
6  security results:  MAC over manifest
7  id.security.src
```

BIB Security Block