draft-ietf-msec-ipsec-multicast-extensions-00.txt

Brian Weis

George Gross

Dragan Ignjatic

Status

- Draft -00 submitted before Paris
- Dragan presented the draft at the Paris meeting
  - Some comments made with respect to anti-replay protection for multi-sender SAs.
- Authors still struggling with scope issues, and seek input from the WG.
  - Discuss now
  - Post issues & discussion on the list after the meeting

Anti-replay protection for multi-sender SAs

- A single-sender IPsec SA can use the rfc2401bis anti-replay counter without further definition required.
- Multi-sender IPsec SAs are problematic.
  - Per-sender anti-replay counters could be used for SAs with a few senders.
  - Anti-replay for group applications having many senders is not straightforward.

Anti-replay protection for multi-sender SAs

- In Paris it was suggested that this topic be addressed in its own I-D.
- Therefore, the authors will not attempt to solve the problem in this document, other than to note that the group policy should define per-sender IPsec SAs instead.
  - Question: In the interests of interoperability should the draft mandate a lower bound for the number of per-sender SAs to be supported?

Background: GSA Structure (RFC 3740)

```
             +------------------+
             |       GCKS       |
             |                  |
             |   REG      REG   |
             |    /  REKEY \    |
             +---/-----|----\---+
                /      |     \
               /       |      \
              /        |       \
             /         |        \
            /          |         \
+----------/------+    |   +------\----------+
|        REG      |    |   |      REG        |
|            REKEY-----+----REKEY            |
|     Sender      |        |      Receiver   |
|             DATA----------DATA             |
+-----------------+        +-----------------+
```

Issue 1: Goal of this document

Option 1: Define a group-wide GSA architecture, resulting in complete interoperability between heterogeneous devices?

- IPsec SAs (including SAD/SPD/PAD definitions)
- Group Key Management (such that different group keying implementations will interoperate)
  - GCKS Registration SA policy
  - GCKS Rekey SA policy

Rationale: Defining requirements on the entire GSA is necessary in order to achieve full group IPsec interoperability between vendors.

Issue 1: Goal of this document

Option 2: Define a group-wide IPsec SA architecture, resulting in IPsec interoperability between heterogeneous devices?

- IPsec SAs (including SAD/SPD/PAD definitions)

Rationale: The rfc2401bis document primarily describes IPsec major databases, and IPsec processing rules for data packets. This document should do the same.

Issue 2: GCKS Deployments

Should this document mandate multiple GCKS devices be defined in this architecture?

Rationale: Multiple GCKS devices are necessary for large groups to operate.

If so, should a single GCKS architecture (e.g., hierarchical key server arrangement) be mandated?

Rationale: A particular arrangement must be mandated in order to ensure interoperability between different vendors.

Issue 3: Composite Cryptographic Groups

- Definition: The logical group formed from union of two or more sub-groups, each sub-group supporting different cryptographic properties.
- Composite groups occur when large-scale groups contains multiple protocol versions or multiple interoperable vendors.
  - e.g. retiring 3-DES, migrating to AES
  - software bug fixes

Motivations for Composite Groups

- Can not easily upgrade a large-scale group, no “flag day” is allowed
- Cryptographic algorithms age or break, need strategy to move to new ones
  - witness recent attacks on MD5, SHA-1
- Parallel vendor-specific sub-groups support different feature sets, want best combination
- Straddle IPv4 and IPv6 sub-groups

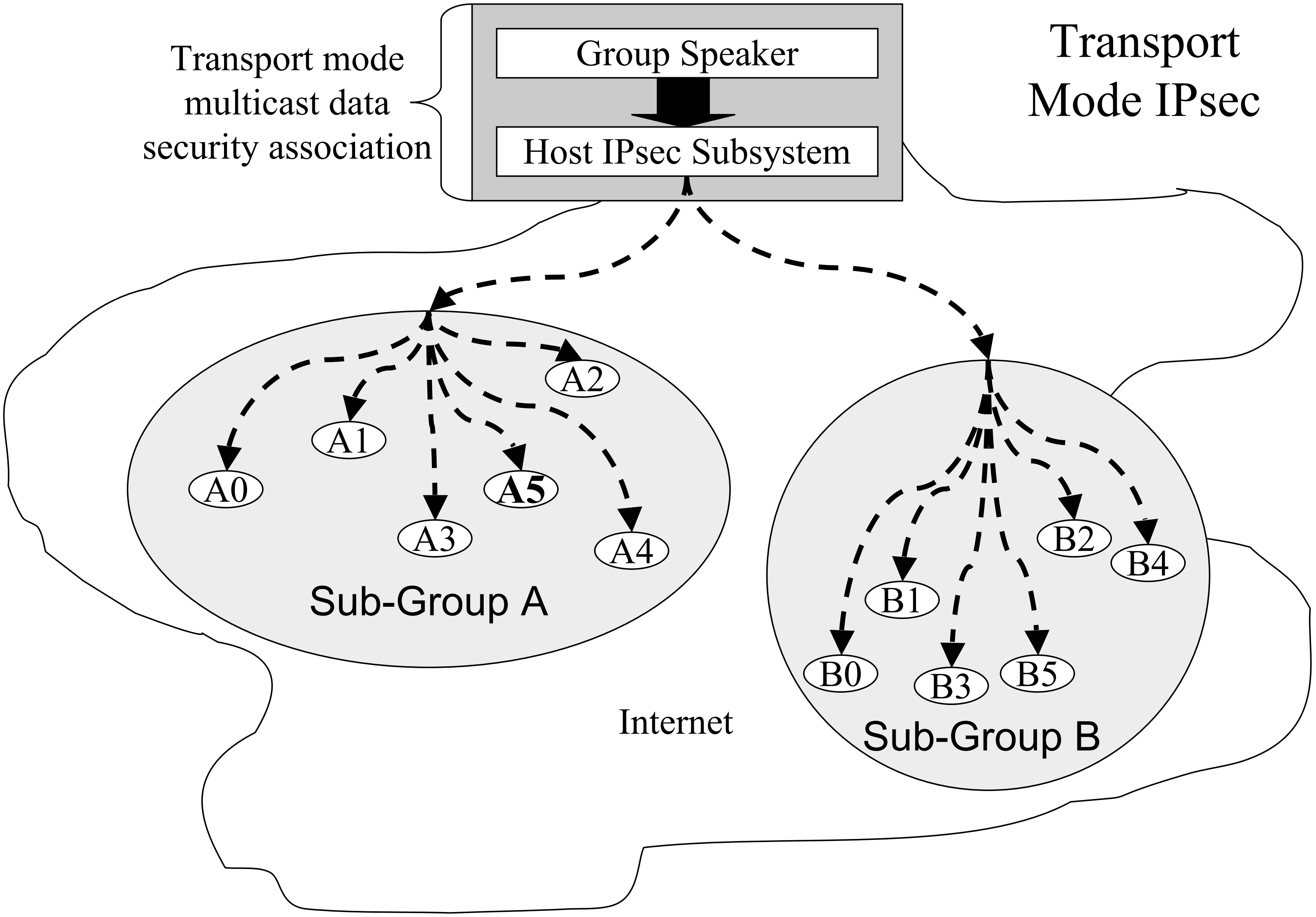
Packet Replication

- A multicast application is unaware of sub-groups, it only sends one packet to the composite group, not each sub-group.
- Therefore, there must be a mechanism where each data packet gets replicated once per sub-group, and treated with the respective sub-group’s IPsec cryptographic policy.
  - IPsec policy is per sub-group, set by its GCKS
- The question is, where should the replication happen?

Composite Group Transport Mode

- Replication happens on the host
  - End-to-end security, no plain-text on wire
  - Supports Native, BITS, and BITW architectural modes
  - Requires IPsec subsystem replicate each data SA packet for each sub-group before applying its cryptographic algorithms
    - do not want multicast application to be aware of the cryptographic sub-groups

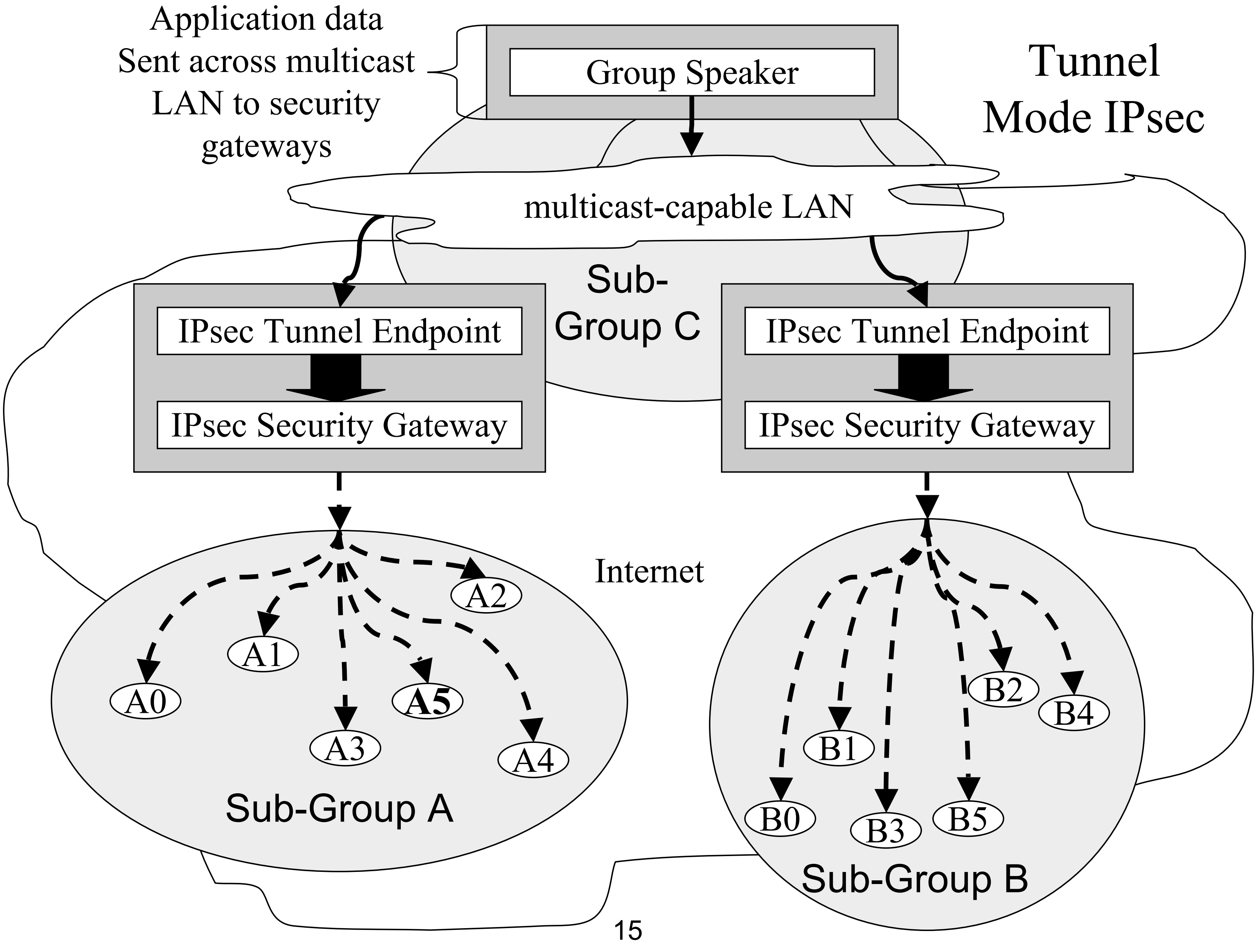
Transport Mode IPsec



Composite Group Tunnel Mode

- Replication happens in the network
  - The application multicasts its data to two or more IPsec security gateways, one gateway per sub-group.
  - Simply bolt together as many gateways as there are sub-groups
  - Traffic may need to be protected between the gateways as well.

Tunnel Mode IPsec



Application data
Sent across multicast
LAN to security
gateways

Issue 3: Composite Groups

Should the document specify new IPsec semantics to support composite groups? E.g., requiring packet replication as part of the IPsec encapsulation processing?

Rationale: Required to support all possible IPsec architectures

Issue 4: GKMS/IPsec interface

Question: Should all GKMPs use the same namespace, as a common interface to IPsec?

Rationale: Doing so would simplify the interface from GKMPs to IPsec, which simplifies the IPsec subsystem.

But first, there’s a meta-question: What is an interface to an IPsec subsystem?

- Policy Token?
- IPsec SA Attributes?
- API?

Next Steps

- Resolve draft scope issues
- Issue -01 before IETF 66 in Dallas
  - The IPsec mailing list will be invited to review this draft.