Group Keying for TRILL Update

draft-ietf-trill-group-keying

Donald E. Eastlake, III

Huawei Technologies

<d3e3e3@gmail.com>

Contents

- **Background on point-to-point and group security**
- **The existing group keying draft**
- **Proposed Changes**
- **Next Steps**

Security

- TRILL standardizes communications protocols that sometimes need encryption and authentication services. Such services require that cryptographic keying material be distributed.
- Modern security standards impose a number of requirements on keying including a limited lifetime on keys.

Security

- Existing TRILL specified security is unicast:
  - Unicast security is pretty simple. You need session keys to exist only at the two end points.
  - TRILL uses existing point-to-point security and pairwise secret key negotiation:
    - RBridge Channel messages: [RFC7178] extended to add DTLS unicast security by [RFC7978].
    - TRILL over IP [draft-ietf-trill-over-ip] unicast IPsec security with IKEv2 key negotiation.

Multicast

- Where multicast / broadcast is supported, it can be inherently more efficient, decreasing link and source port utilization.
  - The RBridge Channel facility inherently supports multi-destination packets scoped by data label (VLAN or FGL).
  - Some IP networks/links support native IP multicast.

Multicast Security

- Possible Approaches
  1. You can just serially unicast to all the intended destinations but you lose the advantages of multicast and need to know who all destinations are.
  2. You can distribute a shared secret key to all the group members. This is efficient but now any group member can forge packets as if they were from another group member

Multicast Security

- Approaches (continued)
  3. You can use public key cryptography with each packet. This supports good encryption and authentication but this is inefficient.
  4. You can perhaps do more exotic things.

TRILL Multicast Security

- The idea is for TRILL to support approach 2, a shared secret key.
- For networks where the diminished authentication of not protecting which group member originated a packet is a problem, they can always fall back to serial unicast.

Contents

- Background on point-to-point and group security
- The existing group keying draft
- Proposed Changes
- Next Steps

Group Keying Protocol

- draft-ietf-trill-group-keying specifies generic messages for a designated group member to distribute shared secret keying material to all other group members.
- Also includes profiles for use of those generic group keying messages for multi-destination
  - RBridge Channel messages
  - TRILL over IP

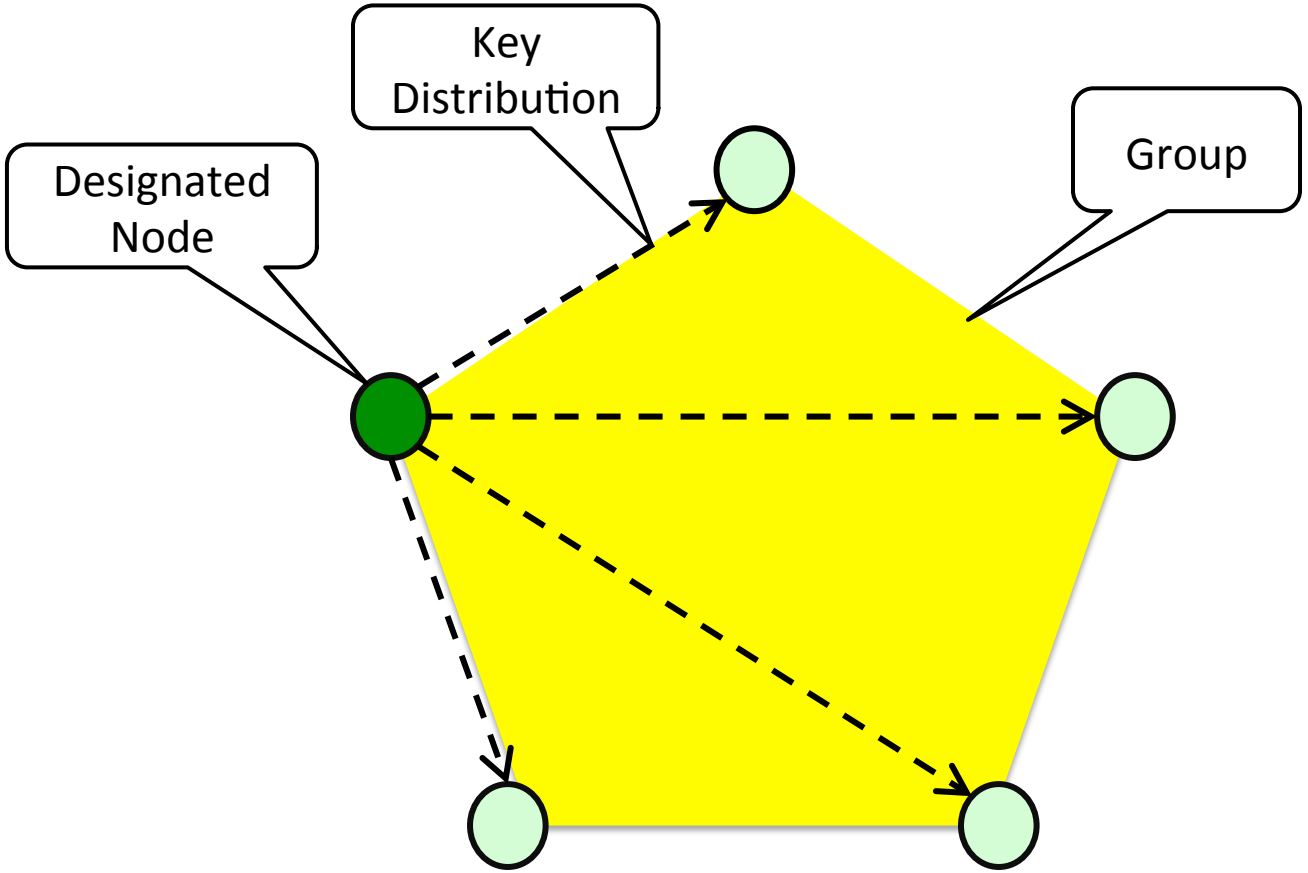
Group Keying Protocol

- draft-ietf-trill-group-keying:
  - Leverages pairwise keying, which it assumes is already in place at least between the designated group member and all other group members.
  - Assumes group keying will be profiled for each application by specification of at least
    - the envelope around the group keying messages.
    - how the designated group member is determined

Group Keying Protocol

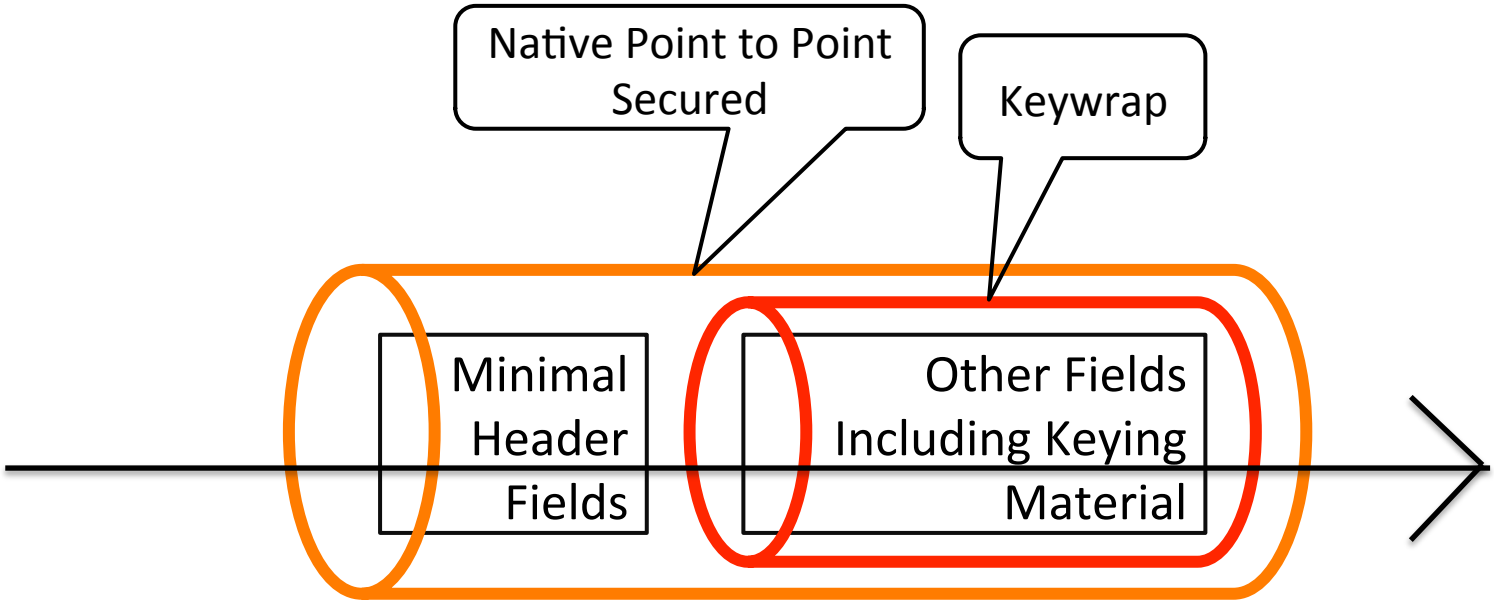
- draft-ietf-trill-group-keying (cont):
  - Provides for key identifiers so you can pre-position the next key before switching to it and deprecating the current key. This avoids a dropout when doing a key rollover.
- Note: All this just relates to keying. The actual secured packet formats and crytogrphic algorithms for encryption and authentication are unchanged.

Group Keying Protocol



Group Keying Protocol

Group Keying
Message Structure



Contents

- Background on point-to-point and group security
- The existing group keying draft
- Proposed Changes
- Next Steps

Proposed Changes

- Split draft into two drafts. The existing draft describes
  - a general group keying mechanism, and
  - gives profiling of that mechanism for group keying for (1) RBridge Channel messages and (2) TRILL over IP packets.
- Add algorithm agility for the key wrap algorithm.
- Finish up profiling for TRILL over IP.

Proposed Changes

- Split draft into two drafts, one with generic group keying mechanism, one with profiling for RBridge Channel messages and TRILL over IP. (Or move TRILL over IP profiling to TRILL over IP draft.)
  - This should make review and any future updates easier.
    - Generic group keying part should probably be last called in SAAG as well as TRILL.

Proposed Changes

- Give inner key wrap algorithm agility.
  - Current uses AES Key Wrap, fixed algorithm
  - It is expected that other Key Wrap algorithms will be standardized, for example a Cha-Cha Key Wrap to protect against possible future problems with AES and because Cha-Cha is much more efficient in software.

Proposed Changes

- Complete TRILL over IP profiling of group key. Currently that section is incomplete.

Contents

- Background on point-to-point and group security
- The existing group keying draft
- Proposed Changes
- Next Steps

Next Steps

- Post to TRILL WG Mailing list asking if there are any objections to
  - Splitting the current draft into generic group keying and TRILL specific drafts
  - Adding algorithm agility for key wrap algorithm

END

Donald E. Eastlake, III
Huawei Technologies
d3e3e3@gmail.com