LISP Data-Plane Confidentiality

draft-farinacci-lisp-crypto-01

LISP Working Group
Toronto IETF
July 2014

Dino Farinacci

Chronology

- Presented ideas in LISP WG in Vancouver **fall 2013**
- Seek advice from SAAG in Vancouver **fall 2013**
- Present -00 draft in London **spring 2014**
- Wrote -00 implementation **spring 2014**
- Present -01 and implementation here in Toronto **summer 2014**

Design Overview

- Diffie-Hellman exchange via Map-Request/Map-Reply
- Keys not stored by third-party
- Keys are ephemeral
- ITR *encrypt-n-encap* -> ETR *decap-n-decrypt*
- Rekeying part of RLOC-probing

Key Exchange

```
11:17:09.865: itr: Receive any/eth0 [0]22.0.0.2 -> [0]33.0.0.3, inner tos/ttl: 0/64, length: 84, packet: 45000054
00004000 400103a5 16000002 21000003 0800f9ec 1c4e0001 24b6ca53 00b70700 08090a0b 0c0d0e0f 10111213 14151617
18191a1b 1c1d1e1f       ...
11:17:09.865: itr: Lookup for EID [0]33.0.0.3 not found in map-cache
11:17:09.866: itr: Map-Request -> flags: adrspimxd, itr-rloc-count: 1 (+1), record-count: 1, nonce:
0x4989b9206a677ba3, source-eid: afi 1, [0]22.0.0.2, target-eid: afi 1, [0]33.0.0.3/32, ITR-RLOCs:
11:17:09.866: itr:   itr-rloc: afi 1 [0]1.0.0.2, g/p/local-key/remote-key: 2/7919/7129/none
11:17:09.866: itr:   itr-rloc: afi 2 [0]2602:306:3a29:6c70:5cff:afe3:109d:173a
11:17:09.866: itr: ECM -> flags: sdem, inner IP: [0]1.0.0.2 -> [0]33.0.0.3, inner UDP: 39107 -> 4342
11:17:09.866: itr: Send Encapsulated-Control-Message to 1.0.0.5


11:17:09.910: itr: Receive 90 bytes from 1.0.0.3 4342, packet: 20000001 a37b676a 20b98949 000005a0 01081000
00000001 21000000 0000ff00 00054003 00000100 00300001 01000003 40030000 0b000022 01000000 00160400 00000208
00001eef 00000000 cb090000 00000000 00010100 0003
11:17:09.910: itr: Map-Reply -> flags: res, record-count: 1, nonce: 0x4989b9206a677ba3
11:17:09.910: itr:   EID-record -> record-ttl: 1440, rloc-count: 1, action: no-action, auth, map-version: 0, afi:
1, [iid]eid/ml: [0]33.0.0.0/8
11:17:09.954: itr:     RLOC-record -> flags: LpR, 0/0/255/0, afi: 1, rloc: 1.0.0.3, g/p/local-key/remote-key:
2/7919/7129/2507
11:17:09.954: itr: Compute shared-key with g/p/local-key/remote-key: 2/7919/7129/2507
11:17:09.954: itr: Add [0]33.0.0.0/8 to map-cache with 1 RLOCs
```

E-n-E then D-n-D

```
11:17:10.507: itr: Receive any/eth0 [0]22.0.0.2 -> [0]33.0.0.3, inner tos/ttl: 0/64, length: 84, packet: 45000054
00004000 400103a5 16000002 21000003 0800afe5 1c4e0003 26b6ca53 48bc0700 08090a0b 0c0d0e0f 10111213 14151617
18191a1b 1c1d1e1f       ...
11:17:10.511: itr: Lookup for EID [0]33.0.0.3 found map-cache entry [0]33.0.0.0/8
11:17:10.512: itr: Packet hash is 0, best-rloc-list: [['1.0.0.3', 'up-state']]

11:17:10.512: itr: Encrypt with shared-key for key-id: 1, g/p/local-key/remote-key: 2/7919/7129/2507, rloc: 1.0.0.3
11:17:10.512: itr: Send LISP packet, outer RLOCs: [0]1.0.0.2 -> [0]1.0.0.3, outer tos/ttl: 0/63, outer UDP: 61925 -
> 4341, inner EIDs: [0]22.0.0.2 -> [0]33.0.0.3, inner tos/ttl: 0/63, length: 132, encrypt/encap LISP-header ->
flags: NlevipK1, nonce: 0x4fb658, iid/lsb: 0x0, packet: 45000084 dfdf0000 3f119985 01000002 01000003 f1e510f5
00700000 814fb658 00000000 b89f2416 fadc4686 bab9f63c bfb0dc55 39d4911d       ...
```

```
11:17:19.574: etr: Receive LISP packet, outer RLOCs: [0]1.0.0.2 -> [0]1.0.0.3, outer tos/ttl: 0/63, outer UDP:
63335 -> 4341, inner EIDs: [0]22.0.0.2 -> [0]33.0.0.3, inner tos/ttl: 0/63, length: 120, decap/decrypt LISP-header
-> flags: NlevipK1, nonce: 0x4fb658, iid/lsb: 0x0, packet: 45000084 dfdf0000 3f119985 01000002 01000003 f76710f5
00700000 814fb658 00000000 45000054 00004000 3f0104a5 16000002 21000003       ...

11:17:20.574: etr: Decrypt with shared-key for key-id: 1, g/p/local-key/remote-key: 2/7919/2507/7129, rloc: 1.0.0.2
11:17:19.580: etr: Forward packet for EIDs [0]22.0.0.2 -> [0]33.0.0.3: 45000054 00004000 3e0105a5 16000002 21000003
080018f7 1c4e000c 2fb6ca53 d5a10800 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f       ...
```

Changes to -01

B.1. Changes to draft-farinacci-lisp-crypto-01.txt

- Posted July 2014.
- Add Group-ID to the encoding format of Key Material in a Security Type LCAF and modify the IANA Considerations so this draft can use key exchange parameters from the IANA registry.
- Indicate that the R-bit in the Security Type LCAF is not used by lisp-crypto.
- Add text to indicate that ETRs/RTRs can negotiate less number of keys from which the ITR/PITR sent in a Map-Request.
- Add text explaining how LISP-SEC solves the problem when a man-in-the-middle becomes part of the Map-Request/Map-Reply key exchange process.
- Add text indicating that when RLOC-probing is used for RLOC reachability purposes and rekeying is not desired, that the same key exchange parameters should be used so a reallocation of a pubic key does not happen at the ETR.
- Add text to indicate that ECDH can be used to reduce CPU requirements for computing shared secret-keys.

Working Group Work Item?

- No consensus in London about making this a WG document
- Requesting at this time to make WG document