LISP Data-Plane Cryptography

draft-ietf-lisp-crypto-01

LISP Working Group - Prague IETF
July 2015

Dino Farinacci & Brian Weis

Document Status

- Presented ideas in LISP WG at Vancouver **fall 2013**
- Seek advice from SAAG at Vancouver **fall 2013**
- Present -00 individual submission draft in London **spring 2014**
  - *lispers.net* implementation **spring 2014**
- Present -01 and implementation
  - Toronto **summer 2014** & Honolulu **fall 2014**
- Created working group draft -00 **Jan 2015**
- Presented update Dallas **spring 2015**
  - Lots of technical discussion on key sizes, cipher suites, IVs, and ICVs
  - Led to -01 update in **May 2015** where security expert added as co-author (Brian)

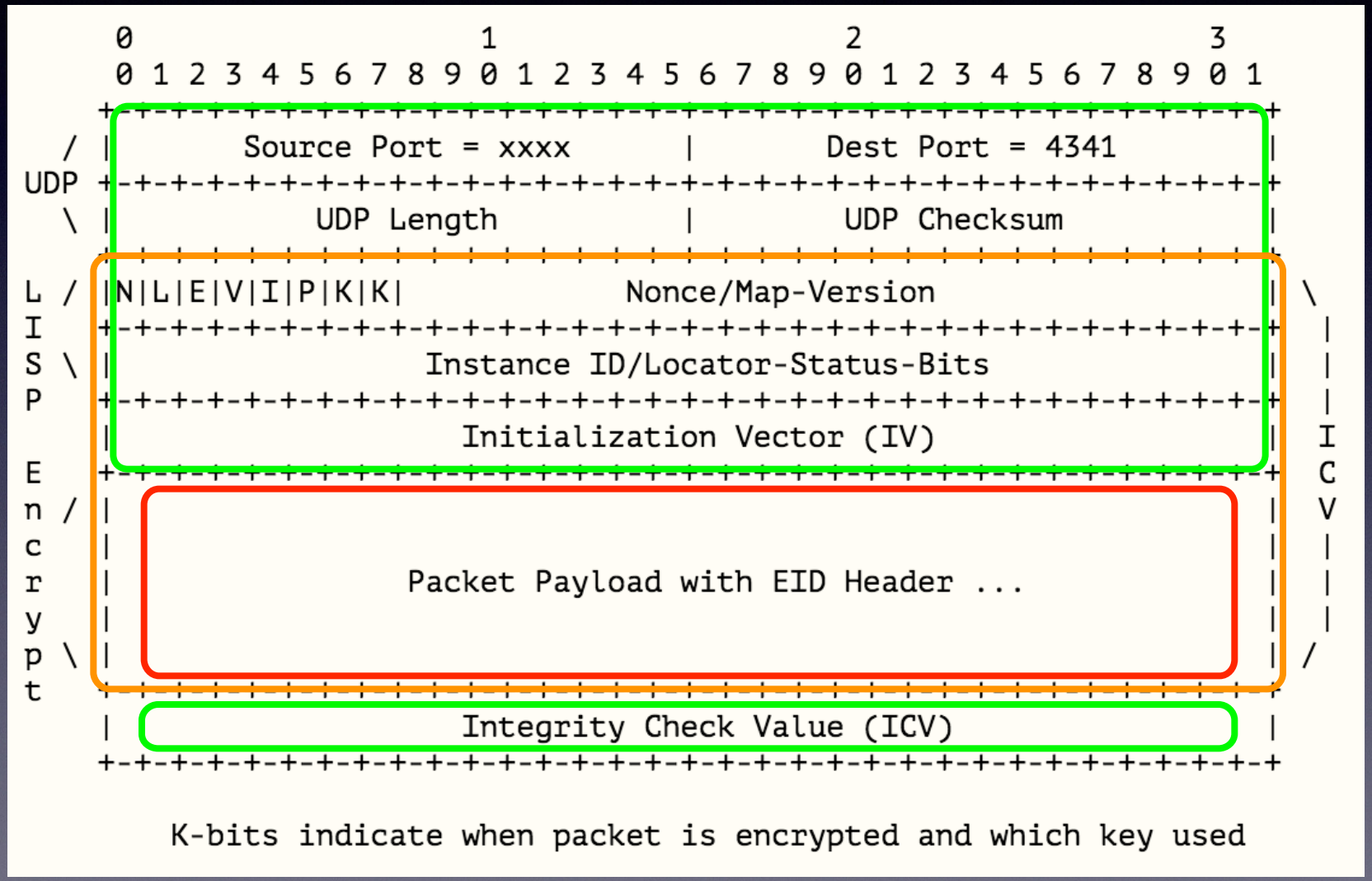
Design Overview

- 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

What We Added in -01

- Initialization Vector (IV) to the start of payload
- Integrity Check Verification (ICV) at end of payload
- Use Authenticated Encryption with Additional Data (AEAD)
- Have DH secret key as input to a KDF that produces an encryption-key and integrity-key
- Add cipher suite values which are negotiated in the Map-Request/Map-Reply exchange

Packet Format



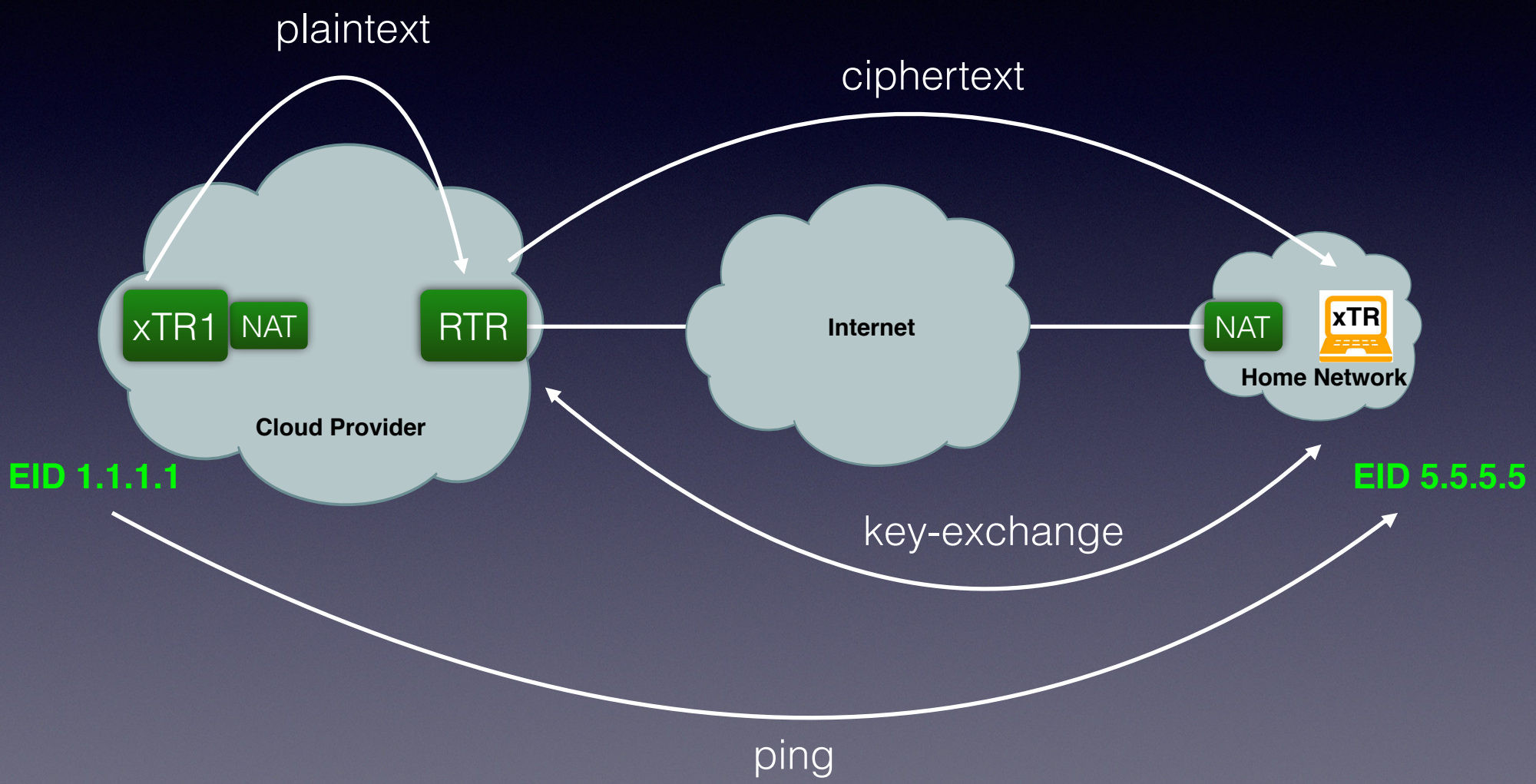
Implementation Status

- *lispers.net* has a -01 implementation

```
Cipher Suite 1:
  Diffie-Hellman Group: 1024-bit Modular Exponential (MODP) [RFC2409]
  Encryption:           AES with 128-bit keys in CBC mode [AES-CBC]
  Integrity:            HMAC-SHA1-96 [RFC2404]
```

- Used ECDH instead of regular DH:
  - RFC5114 *gx* value from the “192-bit Random ECP Group”
- Supports rekeying via RLOC-probing
- Support for unidirectional encryption across NATs
  - RTR to xTR-behind NAT as well as xTR-behind-NAT to RTR

lisp-crypto Example



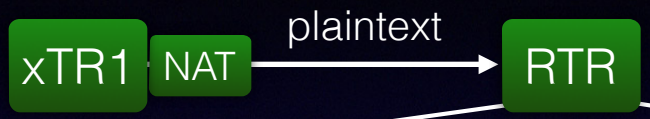
lisp-crypto Key Exchange

```
07/16/15 21:29:57.873: rtr: RLOC-probe 12.130.117.23, last rtt: 0.232
07/16/15 21:29:57.874: rtr: Map-Request -> flags: adRspimxd, itr-rloc-count: 0 (+1), record-count: 1, nonce: 0xf932b78b8892c538, source-eid: afi 0, [0]no-address,
target-eid: afi 1, [255]5.5.5.0/24, ITR-RLOCs:
07/16/15 21:29:57.874: rtr:   itr-rloc: afi 1 [0]10.240.106.249  ECDH cipher-suite: 1, local-key: 0x00000000...0959924c(128), remote-key: none
07/16/15 21:29:57.874: rtr: Data encapsulate RLOC-probe request to 12.130.117.23  dino-macbook  port 3745 for NAT-traversal
07/16/15 21:29:57.874: rtr: Send LISP packet, outer RLOCs: [0]10.240.106.249 -> [0]12.130.117.23, outer tos/ttl: 0/64, outer UDP: 4341 -> 3745, control-packet: 450
000f6 dfdf4000 40116295 0af06af9 0c827517 10f50ea1 00e20000 84db37fd ffffff00 450000d2 00000000 40118299 0af06af9 0c827517       ...
```

```
07/16/15 14:29:58.867: etr: Receive 218 bytes from 130.211.169.66 4341, packet: 84db37fd ffffff00 450000d2 00000000 40118299 0af06af9 0c827517 000010f6 00be0000 12
000001 38c59288 8bb732f9 00004003 00000b00 008c0100       ...
07/16/15 14:29:58.867: etr: Kernel-decap [0]10.240.106.249 -> [0]12.130.117.23, tos/ttl: 0/64, length: 210, packet: 450000d2 00000000 40118299 0af06af9 0c827517 00
0010f6 00be0000 12000001 38c59288 8bb732f9 00004003 00000b00 008c0100 01000080 00000000       ...
07/16/15 14:29:58.867: etr:   LISP-header -> flags: NlevIpk, nonce: 0xdb37fd, iid/lsb: 0xffffff00
07/16/15 14:29:58.868: etr: New keying for RLOC 130.211.169.66
07/16/15 14:29:58.868: etr: Compute shared-key for RLOC 130.211.169.66, nonce 0xf932b78b8892c538 ...
07/16/15 14:29:58.868: etr: Computed shared-key  0x00000000...10b8d188(128)
07/16/15 14:29:58.868: etr: Computed encryption and integrity check keys
07/16/15 14:29:58.868: etr: Map-Request -> flags: adRspimxd, itr-rloc-count: 0 (+1), record-count: 1, nonce: 0xf932b78b8892c538, source-eid: afi 0, [0]no-address,
target-eid: afi 1, [255]5.5.5.0/24, ITR-RLOCs:
07/16/15 14:29:58.868: etr:   itr-rloc: afi 1 [0]130.211.169.66  ECDH cipher-suite: 1, local-key: 0x00000000...5153880c(128), remote-key: 0x00000000...0959924c(128
)
07/16/15 14:29:58.868: etr: Received RLOC-probe Map-Request, send RLOC-probe Map-Reply
07/16/15 14:29:58.868: etr: Found database-mapping EID-prefix [255]5.5.5.0/24 for requested EID [255]5.5.5.0/24
07/16/15 14:29:58.868: etr: Map-Reply -> flags: Res, record-count: 1, nonce: 0xf932b78b8892c538
07/16/15 14:29:58.868: etr:   EID-record -> record-ttl: 24 hours, rloc-count: 1, action: no-action, auth, map-version: 0, afi: 1, [iid]eid/ml: [255]5.5.5.0/24
07/16/15 14:29:58.869: etr:     RLOC-record -> flags: LPR, 0/0/255/0, afi: 1, rloc: 12.130.117.23, rloc-name: 'dino-macbook', ECDH cipher-suite: 1, local-key: 0x00
000000...5153880c(128), remote-key: 0x00000000...0959924c(128)
07/16/15 14:29:58.869: etr: Data encapsulate RLOC-probe reply to 130.211.169.66 port 4341 for NAT-traversal
07/16/15 14:29:58.870: etr: Send LISP packet, outer RLOCs: [0]172.19.131.126 -> [0]130.211.169.66, outer tos/ttl: 0/64, outer UDP: 64060 -> 4341, control-packet: 4
500011f dfdf4000 4011fe46 ac13837e 82d3a942 fa3c10f5 010b0000 840b2615 ffffff00 450000fb 00000000 40111e4b ac13837e 82d3a942       ...
```

```
07/16/15 21:29:58.105: rtr: Receive-(pcap-0) LISP packet, outer RLOCs: [0]12.130.117.23 -> [0]10.240.106.249, outer tos/ttl: 96/39, outer UDP: 29543 -> 4341, contr
ol-packet: 4560011f dfdf4000 27117b0c 0c827517 0af06af9 736710f5 010b0000 840b2615 ffffff00 450000fb 00000000 40111e4b ac13837e 82d3a942       ...
07/16/15 21:29:58.105: rtr: Map-Reply -> flags: Res, record-count: 1, nonce: 0xf932b78b8892c538
07/16/15 21:29:58.110: rtr:   EID-record -> record-ttl: 24 hours, rloc-count: 1, action: no-action, auth, map-version: 0, afi: 1, [iid]eid/ml: [255]5.5.5.0/24
07/16/15 21:29:58.110: rtr: New keying for RLOC 12.130.117.23
07/16/15 21:29:58.110: rtr: Compute shared-key for RLOC 12.130.117.23, nonce 0xf932b78b8892c538 ...
07/16/15 21:29:58.110: rtr: Computed shared-key  0x00000000...10b8d188(128)
07/16/15 21:29:58.110: rtr: Computed encryption and integrity check keys
07/16/15 21:29:58.111: rtr:     RLOC-record -> flags: LPR, 0/0/255/0, afi: 1, rloc: 12.130.117.23, rloc-name: 'dino-macbook', ECDH cipher-suite: 1, local-key: 0x00
000000...0959924c(128), remote-key: 0x00000000...5153880c(128)
07/16/15 21:29:58.111: rtr:       Store translated encap-port 3745 for RLOC 12.130.117.23, rloc-name 'dino-macbook'
07/16/15 21:29:58.111: rtr:       Received RLOC-probe reply from 12.130.117.23/3745, state-change up-state -> up, new rtt 0.237
07/16/15 21:29:58.111: rtr:       Update RLOC-probe state for [255]5.5.5.0/24
07/16/15 21:29:58.111: rtr: Replace [255]5.5.5.0/24 to map-cache with 1 RLOCs
```

lisp-crypto Encrypt/Decrypt




```
07/16/15 21:29:58.417: rtr: Receive-(pcap-0) LISP packet, outer RLOCs: [0]104.154.81.79 -> [0]10.240.106.249, outer tos/ttl: 96/56, outer UDP: 61440 -> 4341, inner
 EIDs: [255]1.1.1.1 -> [255]5.5.5.5, inner tos/ttl: 0/63, length: 120, decap LISP-header -> flags: NlevIpk, nonce: 0x8b377f, iid/lsb: 0xff00, packet: 45600078 dfdf
4000 38113263 689a514f 0af06af9 f00010f5 00640000 848b377f 0000ff00 45000054 315b0000 3f013e43 01010101 05050505       ...
07/16/15 21:29:58.417: rtr: Lookup for EID [255]5.5.5.5 found map-cache entry [255]5.5.5.0/24
07/16/15 21:29:58.417: rtr: Packet hash is 0, best-rloc-list: [['12.130.117.23', 'up-state']]
07/16/15 21:29:58.417: rtr: Encrypt for key-id: 1, RLOC: 12.130.117.23, ICV: 0x5489a85a...b63b7a65
07/16/15 21:29:58.418: rtr: Send LISP packet, outer RLOCs: [0]10.240.106.249 -> [0]12.130.117.23, outer tos/ttl: 0/56, outer UDP: 4341 -> 3745, inner EIDs: [255]1.
1.1.1 -> [255]5.5.5.5, inner tos/ttl: 0/56, length: 168, encrypt/encap LISP-header -> flags: NlevIpK1, nonce: 0xffb77f, iid/lsb: 0xff00, packet: 450000a8 dfdf4000
38116ae3 0af06af9 0c827517 10f50ea1 00940000 85ffb77f 0000ff00 17520b89 e02073c3 8a1b3c70 68457419 edc9ff9d       ...
```


```
07/16/15 14:29:59.411: etr: Receive 140 bytes from 130.211.169.66 4341, packet: 85ffb77f 0000ff00 17520b89 e02073c3 8a1b3c70 68457419 edc9ff9d 09350c4a cebf6db4 94
fc1b0c bd0c6784 b6551175 64d81105 f909de5c 79980cd9       ...
07/16/15 14:29:59.411: etr: Decrypt for key-id: 1, RLOC: 130.211.169.66, ICV: 0x5489a85a...b63b7a65 (good)
07/16/15 14:29:59.412: etr: Kernel-decap [255]1.1.1.1 -> [255]5.5.5.5, tos/ttl: 0/62, length: 84, packet: 45000054 315b0000 3e013f43 01010101 05050505 0000cd75 e65
5abec 55a82257 00023d43 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f       ...
07/16/15 14:29:59.412: etr:   LISP-header -> flags: NlevIpK1, nonce: 0xffb77f, iid/lsb: 0xff00
07/16/15 14:29:59.412: etr: NAT-Forward packet for EIDs [255]1.1.1.1 -> [255]5.5.5.5: 45000054 315b0000 3e013f43 01010101 05050505 0000cd75 e655abec 55a82257 00023
d43 08090a0b 0c0d0e0f 10111213 14151617 18191a1b 1c1d1e1f       ...
```

Implementation Todo List

- Key Related Testing
  - Larger keys, other ECDH groups, and other ciphers
  - Multi-key rekeying logic
- Multi-Feature Testing
  - Test multicast in unicast encapsulation
  - Test with LISP-SEC
- Interoperability Testing
  - Making a call for more implementations
  - How about ***lispmob*** and open source the code?

Questions?