LISP Data-Plane Confidentiality

draft-ietf-lisp-crypto-00

LISP Working Group
Dallas IETF - March 2015

Dino Farinacci

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**

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

Jan 2015 Discussions

- WG can discuss security specific encapsulation format details
  - LISP-GPE may have a more general encoding
- WG needs to detail out interaction with LISP-SEC & LISP-DDT-SEC
  - To cover MITM attacks
- Doing ECDH will cause MTU problems packing 3 large keys in Map-Requests/ Map-Replies
- Reduce the number of options (Watson Ladd - crypto experts)
  - Even though WG wanted more flexible security option negotiation
- Other Watson comments:
  - Thought re-keying logic was good
  - Wanted the draft to discuss security structure of the mapping database - but more of a general LISP architecture comment

Implementation Todo List

- Key Related Testing
  - Larger keys, ECDH, and other ciphers
  - Rekeying logic
- Multi-Feature Testing
  - ITR to RTR testing, including NAT-traversal
  - 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?