

Update on LISP Security

~~draft-saucez-lisp-security-01.txt~~
~~draft-saucez-lisp-security-02.txt~~
draft-saucez-lisp-security-03.txt

Luigi Iannone
Damien Saucez
Olivier Bonaventure

Main changes:

- Editorial polishing
 - Few sections re-ordering and re-titling
 - Figures update
- Terminology update
 - E.g., LISP Database => EID-to-RLOC Database
- Clarified the Map-Request amplification attack
- Added section about Interworking
- References update

Interworking: Proxy-ITR



- Check on source EID
 - No EID-to-RLOC Database on PITRs
 - Firewall/ACL to limit encapsulation of unwanted traffic
- Check on destination EID
 - Static EID-to-RLOC Cache entries only for customers
 - On cache-miss drop packet and do not send Map-Request

Interworking: Proxy-ETR



- Check on source EID
 - Static EID-to-RLOC Cache only for customers
 - On cache-miss drop packet and do not send Map-Request
 - Drop packet when source RLOC not valid

Next Steps...

- Review from security experts
- Integrate further comments (if any)
- Finalize and include missing parts (e.g. LISP-MS)