LISP-SEC

draft-ietf-lisp-sec-14

F. Maino, V. Ermagan, A. Cabellos, D. Saucez

IETF 100 - Singapore

LISP-SEC Moved to Standards Track

From: BRUNGARD, DEBORAH A
To: lisp@ietf.org
Subject: RE: Datatracker State Update Notice: <draft-ietf-lisp-sec-13.txt>

LISP,
I've pulled this document off the upcoming telechat and returned it to the working group after talking with your Chairs and the Authors. We had an **OPS-DIR review** which **questioned why we don't take this document standards-track.** But as it has references to 6830 and 6833, it can not be PS. But when the bis documents are done, we may then have difficulties as this one is Experimental.

The **bis documents are making excellent progress, so we'll progress all three documents together as PS.** This will let us have the flexibility to handle the DIR reviewers/IESG comments by determining which document is more appropriate.

Thanks and keep up the progress on the bis documents!

Deborah

Changes Since rev-12

- All changes were introduced in the “Security Considerations” section to address the last call review
  1. Recommendation to periodically refresh LISP-SEC shared keys to address key aging and key compromise
  2. Clarification on resiliency to Replay Attacks based on use of nonce
  3. Considerations on role of LISP-SEC to mitigate DoS and DDoS

Changes Since rev-12 (cont)

6.5. Shared Keys Provisioning

Provisioning of the keys shared between the ITR and the Map-Resolver as well as between the ETR and the Map-Server should be performed via an orchestration infrastructure and it is out of the scope of this draft. It is recommended that both shared keys are refreshed at periodical intervals to address key aging or attackers gaining unauthorized access to the shared keys. Shared keys should be unpredictable random values.

6.6. Replay Attacks

An attacker can capture a valid Map-Request and/or Map-Reply and replay it, however once the ITR receives the original Map-Reply the <nonce,ITR-OTK> pair stored at the ITR will be discarded. If a replayed Map-Reply arrives at the ITR, there is no <nonce,ITR-OTK> that matches the incoming Map-Reply and will be discarded.

In case of replayed Map-Request, the Map-Server, Map-Resolver and ETR will have to do a LISP-SEC computation. This is equivalent to a valid LISP-SEC computation and an attacker does not obtain any benefit.

6.7. Denial of Service and Distributed Denial of Service Attacks

LISP-SEC mitigates the risks of Denial of Service and Distributed Denial of Service attacks by protecting the integrity and authenticating the origin of the Map-Request/Map-Reply messages, and by preventing malicious ETRs from overclaiming EID prefixes that could re-direct traffic directed to a potentially large number of hosts.

Asks

- Move LISP-SEC back to last call?

Thanks!