Update on LISP Security

~~draft-saucez-lisp-security-01.txt~~
~~draft-saucez-lisp-security-02.txt~~
~~draft-saucez-lisp-security-03.txt~~
draft-ietf-lisp-threats-00.txt

Damien Saucez
Luigi Iannone
Olivier Bonaventure

Main changes

- Editorial polishing
  - typos
  - rephrasing
  - nomenclature consolidation (with LISP-Sec draft)
- Added new threats
  - instance ID
  - Map-Server
  - Map-Resolver
- Added filtering recommendation
  - decapsulate only if destination EID downstream the ETR
  - encapsulate only if source EID downstream the ITR
- References update

New threats

- Instance ID
  - forging instance ID to access EID that should not

- Map-Server
  - danger of key sharing
  - registration of invalid RLOC
  - registration of invalid EID prefix

- Map-Resolver
  - MR can become relay attack node
  - cache poisoning (proxy mode)

Next Steps...

- Negative mapping entries discussion (be patient, next slides)
- We tried to document all the categories of attack against LISP, any other?
- Integrate further comments (if any)

Negative mapping entries discussion

- Negative mappings: inform about destination IP prefixes that are not EIDs

- Jeff's mail about DoS attack to fill ITR's cache

  - if many holes in the EID space
    - foreach `hole`
      - attacker.distributed_send_forged (`hole`, via `xTR`)

  - Result: xTR installs the negative mappings and thus fills the cache and/or the cache management "bus"

Negative mapping entries discussion

- Our reply: more general than security => cache management
  - Robert's gave an example going in our direction
  - we propose to add this sentence in the next version of the draft:

```
In addition, an attacker can perform EID-to-RLOC Cache overflow
attack by de-aggregating (i.e., splitting an EID prefix into
artificially smaller EID prefixes) either positive or negative
mappings.
```

- Proposed Solutions (not to be included in this document)
  - overlapping mappings (Jeff)
  - distributed encapsulation via proxies (Robert)
  - cache segmentation/implementation tricks (Noel et al.)
- So what?