A proposal for LISP Security

Sam Hartman

Painless Security, LLC

IETF 76

November 12, 2009

LISP SECURITY

- ➜ `http://tools.ietf.org/wg/lisp/trac/wiki/Security01`
- ➜ Sketch, mostly focuses on control plane
- ➜ `draft-saucez-lisp-security`
- ➜ Mostly focuses on data plane

RECOMMENDED READING

Internet Threats:

BCP 72	BCP 84

Mobile and multi-homing Security:

RFC 4218	RFC 4225
RFC 4219	draft-bagnulo-lisp-threat-01

Goals of LISP Security

Proposed Goals

- ➜ LISP will not make Internet security worse
- ➜ LISP will not create an architecture in which ongoing IETF-wide security goals such as the SIDR working group or BCP 84 are made more difficult.

Key Questions:

- ➜ What does it mean to make security worse?
- ➜ What is our current security model?

Using these Goals

These goals focus the discussion around what in LISP could decrease Internet security or on what ongoing security efforts would be affected. We should be able to answer these questions when proposing LISP security work:

- ➜ What prevents the attack on the Internet today?
- ➜ What is previous IETF thinking about the attack?
- ➜ What are the consequences of the attack?

Control Plane

SECURITY GOALS OF CONTROL PLANE

- ➜ Protect integrity of mapping data
- ➜ Prevent an off-path attacker from appearing as an on-path attacker
- ➜ Limit scope of replays
- ➜ Prevent DOS of the mapping system or caused by the mapping system

End-to-End Cryptography Not the Answer

- Cryptographic verification of Internet-scale mapping information is likely to be difficult. We do not want all ITR and ETR implementations to pay this cost.
- We've found that offloading this functionality is valuable (DNS, PKIX)
- We want sufficient security for our experiments; we don't have end-to-end cryptography today.
- Mandating use of cryptographic security everywhere would be heavy-weight; we need something when it is not used.

Layers of Security

While we will want signed mapping data eventually, we also want to look at these layers.

- ➜ ITR to map resolver
- ➜ Mapping core
- ➜ map server to ETR
- ➜ ETR to ITR

A Sample Attack

MAP REPLY DELEGATION INTEGRITY

How does this approach work in practice? Let's consider a potential attack.

- ➜ The ETR replies directly to the ITR.
- ➜ The ETR tells the ITR how large its prefix is; it can lie. Perhaps even claiming 0::0/0
- ➜ Nonce means that the ITR knows the right ETR is replying; however the ITR shouldn't have to trust that ETR beyond its own delegation.

Is this an attack?

Why is this worse than what we have today? It extends the trust from core routers to each edge router. Any compromise can be an attack on the entire mapping system.

What stops this today? Route filters, relationships between providers, not trusting leaf edge sites to inject routes.

Previous IETF thinking suggests this is a valid problem.

Proposed Requirement

The LISP mapping system MUST provide the ITR with assurance that an ETR is not claiming a prefix larger than one it would be permitted to register. The mapping system MUST provide assurance to an ETR that the prefix in a map reply from the ITR is not larger than the ITR would be permitted to register.

Data Plane

Data Plane Issues

`draft-saucez-lisp-security` begin an exploration of the data plane

- ➜ Address Spoofing
- ➜ Cache poisoning
- ➜ Data integrity
- ➜ Locator reachability
- ➜ Denial of service