Homenet Security

Ted Lemon - *Barefoot Consulting*

Topics

- Babel security document
- Homenet security architecture
- Additional work

Homenet Babel Security

- -00 version of document submitted
- Provides a mechanism for trusting some babel routers and not others
- Identifies which server sent packet
- Works for multicast and unicast (separate mechanisms)
- Relies on HNCP for trust establishment

Specification details

- Public key (ECDSA) for multicast
- Shared secret for unicast, established using DTLS
- Shared secret keys are shared between pairs, not generally
- Spec is basically complete, probably needs to be reviewed and tested
- Did anybody read? Is there interest in working on this?

Homenet Security Architecture

- We need a doc that describes the actual security architecture of the homenet
- Issues:
  - How is perimeter established
  - What kind of perimeter security exists by default
  - How is trust established (how do we designate new router A "trusted" without allowing bad router B to join and be trusted)?
  - How are DNS lookups secured?
  - How do we protect service publication?
  - How do we protect OAM connections (HTTP or whatever)?

Perimeter establishment (current thinking)

- Every router that's doing HNCP is within the perimeter
- Any route that we get outside of HNCP (e.g. with DHCP PD or some other mechanism) is an uplink
- LLNs are distinguished from uplinks because the LLN gateway knows they are special; LLN gateway has to deal with routing from/to LLN, or with LLN aggregation, or however that LLN is operated

Perimeter Security

- Firewall that mimics NAT behavior?
- Do we have prior art to point to?
- Current state of the art: RFC 6092
- Do we need different behavior?
- Do we need changes to support multiple uplinks?
- Should we support MUD and PCP? Do we need to document this?

Establishing Trust

- What keying mechanism?
- How do we decide that a particular key is trusted?
- Current thinking:
  - publish keys using HNCP
  - one or more trust establishment rituals

Securing DNS Lookups

- Would be nice to use DNSSEC for this
- We don’t have a way to do delegations that makes sense in a homenet context
- Options:
  - Come up with a way to automatically get a delegation from the upstream that we can use for trust delegation
  - Come up with a way to trust particular instances of home.arpa

Protecting service publication

- Two problems:
  - How to secure mDNS publications
  - How to secure DNSSD-over-DNS publications
- mDNS: all we have is link security
- DNS: use ToFU as in draft-sctl-service-registration
- There’s a long tail here, since there are no implementations of service registration yet

How do we protect OAM?

- OAM possibilities:
  - an API that apps talk to
  - a web page over https
- API could allow for some way to establish trust as described earlier
- Web PKI absolutely requires a way to get a PKI cert, or else changes to web browsers to support some other mechanism.
  - The only such other mechanism would be TLSA, but that seems not to be happening
  - PKI cert currently requires global domain name + ACME

Question #1

- What have I missed here?
- Anything here that doesn’t belong?

Documents to write

- Homenet Security Architecture
- Establishing Homenet Perimeter (maybe this is just a section in architecture)
- Homenet Perimeter Security (can we just reference RFC 6092 with tweaks in the architecture, or is this a new document?)
- HNCP Public Key extension document (or just update HNCP?)
- Homenet Trust Establishment Rituals
- Establishing a public DNS delegation for homenets
- ToFU DNSSEC trust anchors for homenets
- PKI establishment for homenets
- ???

Question #2

- Does the working group want to do this work?
- Does anybody want to actually work on it?