Homenet Naming and Service Discovery Architecture

Ted Lemon <ted.lemon@nominum.com>

Document changes

Took out a lot of detail that belongs in other documents

Came up with a way forward regarding DNSSD mDNS hybrid solution

Document generally represents what I want out of a homenet naming architecture at this point

Design team/working group participation

Design team hasn’t really coalesced, possibly my fault

Updated document on my own based on comments from several sources

Don’t know whether document is what people want, or just nobody’s complaining

Document as it exists motivates a substantial amount of new work

Do people want this work done/want to do this work?

Hybrid mDNS/DNSSD: *problems*

Link names don’t match naive model of network: not ideal

Name collisions unlikely, but must be handled

No definite way to tell name conflict from multi-homed host

No security at all

Hybrid mDNS/DNSSD: solution overview

Provide a new, “secure” way of doing updates for homenet-aware devices that provide services

Assume that all DNSSD *clients* can do RFC6763 (afawk, they do)

Homenet uses mDNS to defend names registered using DNS update

Homenet-aware devices do not advertise using mDNS

mDNS legacy services

Non-homenet-aware DNSSD devices still use mDNS

mDNS-advertised names are presented as an overlay in DNS, RFC6763-style

Link-local mDNS still functions

Hostname conflicts will be displayed with (x) after the name, e.g. if two devices claim “foo” on different links, UI will show foo(1) and foo(2).

Or maybe foo-1 and foo-2.

Not perfect, but most of the time this will be the same host on two links.

No worse in the case of conflict than defending names across links.

New documents that need to be written

Security architecture

Management API

Homenet global name registration API/process

2-3 other naming documents

Security

This architecture presumes the existence of security which doesn't actually exist or at least isn't documented.

We need to do a security architecture document

We talked a lot a couple of years ago about how to bootstrap trust without demanding too much of the user. We need to turn that discussion into a document sooner rather than later, or at least figure out what the security profile looks like without that.

Management

I think that homenets should probably be manageable using an application or web UI

This should be possible for an intelligent but not knowledgeable end user

IETF should define the management API, or else we'll get proprietary apps with stupid lock-in and a usability nightmare

This needs to happen soon

Standards work on DNS/mDNS/DNSSD

We need to document how mdns and dnssd work on homenets

We need to document how DNS works on homenets

We need to document how DNS on homenets interacts with the outside world (draft-migault-homenet-*?)

We need to document how global names are acquired/registered

In conclusion

If we are going in the wrong direction, now is the time to say so

If you want to work on any of these docs, now is the time to say so

If nobody wants to work on this, it might not happen