DNSSD Discovery Proxy
DNSSD Relay
DNSSD SRP

Ted Lemon <mellon@fugue.com>
Stuart Cheshire <cheshire@apple.com>

Discovery Proxy implementation report

- We have a clean, fully-featured DNSSD Discovery Proxy
- Apache 2.0 license
- Uses mDNSResponder for mDNS and DNS resolution
- Listens on port 53 for regular DNS queries
- Listens on port 853 for DNS Push connections
- Serves as an authoritative server for proxied links
- Serves as a recursive resolver for other queries
- In other news, MacOS Catalina and friends support DNS Push.

DNSSD Discovery Proxy

- Comments/questions?

DNSSD Discovery Relay

- This is intended mostly for situations where DHCP relay would make sense
- Document has not been updated recently
- It has been suggested that this would be easily addressed with a tunneling protocol
- That’s true, but not always easy to configure, particularly in the sense that tunnels are general, and can tunnel traffic that shouldn’t be tunneled.
- So we think there is value in this approach
- How do we get to publication?
- If this WG doesn’t care about this, we could try ISE?
- We should ask on the list.

Discovery Relay implementation

- Code is in an outdated branch of mDNSResponder on the IETF hackathon github repo
- The code works, and much of it has been integrated into mDNSResponder for DNS Push (more on that later)
- I have a new version that is not yet ready for use, but is based on the newer dnssd-proxy/dnssd-srp code base
- This should get pushed out before Singapore

Discovery Relay

- Comments/questions?

SRP Updates (to the document)

- services.arpa -> service.arpa
- Add support for TLS (thanks for suggesting this, Tom)

Tom's comments

- The term "update" is overloaded
  - Right now "update" means both "SRP Update" and "RR update."
  - Tom found this confusing, and it's pretty obvious why now that he's pointed it out.
  - I think we need to use a new name, either "RR Update" or "RR Add." Thotz?
- Tom also found the discussion of validation somewhat confusing generally. I need to fix this, but have not yet done so. I think it's fairly clear what to do.

Tom on Security

- Tom asked if we can support TLS; I think this makes sense and have added TLS support.
- Should we *require* TLS?

Tom on Security 2

- Anycast routing:
  - currently we have a global anycast address
  - this means an SRP update can escape to the Internet
  - We should prevent this
- Possible solutions:
  - A site-scoped anycast address
  - Make this a transport-specific feature
    - e.g., Thread could define a well-known mesh-local address for this.
- Thotz?

Sleep Proxy

- Tom points out:
  - SRP is a routed unicast protocol
  - Sleep Proxy requires a presence on-link
- Sleep proxy was included in SRP because it’s very similar
- But it’s not the same
- Either we need to add some more text explaining this, or
- Make Sleep Proxy a separate document
- Thotz?

Implementation Report

- I have an implementation of the constrained SRP protocol which fits nicely on a small 802.15.4 development board
- Total size of the code is <10k, including key generation and ECDSA SIG(0) signing
- This is a very simple service registration, for a single service.
- Registration, including signature, is about 320 bytes.

SRP Proxy

- Listens for DNS updates on port 53
- Validates them as legitimate SRP updates
- Performs required DNS update(s) to do the SRP update.
- Best cases: new or no change: 1 message
- If a service instance has been removed or added,
  - add the service instances
  - then the host record and PTR records
  - We first try to refresh, then add new
- If any of these fail, we have to delete everything we added
- It all seems to work (I think I tested all the possible cases)

Future Work

- Homenet integration
  - HNCP link identification generation
  - Packages for OpenWRT
  - Default install on OpenWRT that actually works
- Fully-featured SRP client
  - Would need to discover the dnssd-srp-tls.* SRV RR
  - Would need to set up communication over TCP or TLS
  - Otherwise it's pretty similar to srp-simple, but would be nice to make it more general
- SRP in a DNS auth server
  - Some work Mark Andrews has done should enable this
  - I'm hoping to get around to hacking this before Singapore, but no promises.
- SRP Relay
  - This might be a nice thing to have if we wind up using a link-local anycast address for srp-simple

Future of SRP

- The document got one review during last call (Thanks, Tom!)
- The chairs decided this wasn't enough!
- We had a homenet informal meeting on Tuesday, and I asked the folks in the room, who are working on DNS for homenet, whether they thought SRP was useful. Answer: yes. Why didn't they respond to last call? They didn't see it.
- I do not think it makes sense to just drop this work—it's an essential piece of the DNSSD puzzle.
- Therefore I propose that after I update the document again, we do another last call, and include homenet and perhaps DNSOP in the announcement.

DNSSD SRP
DNSSD Relay

Ted Lemon <mellon@fugue.com>
Stuart Cheshire <cheshire@apple.com>

https://github.com/IETF-Hackathon/mDNSResponder