Discovery of Oblivious Services via Service Binding Records

draft-ietf-ohai-svcb-config-01

Tommy Pauly, Tiru Reddy
OHAI
IETF 116, March 2023, Yokohama
Recap

*Target service works with an Oblivious Gateway for OHTTP access (generally co-located)*
Updates in -01

Rename SVCB parameter to "ohttp"

Rename well-known URI to be "ohttp-gateway"

Clarify DoH / DDR behavior
Examples

DNS response (SVCB/HTTPS)

svc.example.com. 7200 IN HTTPS 1 (alpn=h2 ohttp)

_dns.resolver.arpa 7200 IN SVCB 1 doh.example.net (alpn=h2
dohpath=/dns-query{?dns} ohttp)

Oblivious gateway location

https://svc.example.com/.well-known/ohttp-gateway

Key configuration query

GET /.well-known/ohttp-gateway HTTP/1.1
Host: svc.example.com
Accept: application/ohttp-keys
DoH / DDR behavior

OHTTP simply wraps DoH (*DoOH*?)

OHTTP messages sent to gateway uses binary HTTP

Binary HTTP contains "application/dns-message" messages for DoH

If the DoOH server is discovered using _dns.resolver.arpa_ (DDR), the server cert needs to be validated

Easiest way is to check the cert when fetching the key configuration on the well-known location

This check likely needs to be proxied
Next steps: consistency

Key consistency

Key is looked up using well-known URI

Double-check approach (GET proxy & CONNECT proxy)

Check-with-relay approach

"dohpath" consistency

Can limit to the "default" URI of "/dns-query"

Double-check approach (resolve via two methods)

Check-with-relay approach
Next steps

Any other issues beyond consistency?