

IETF Hackathon: DNS/DNSSEC/ DNS Privacy

IETF 102
14-15 July, 2018
Montreal



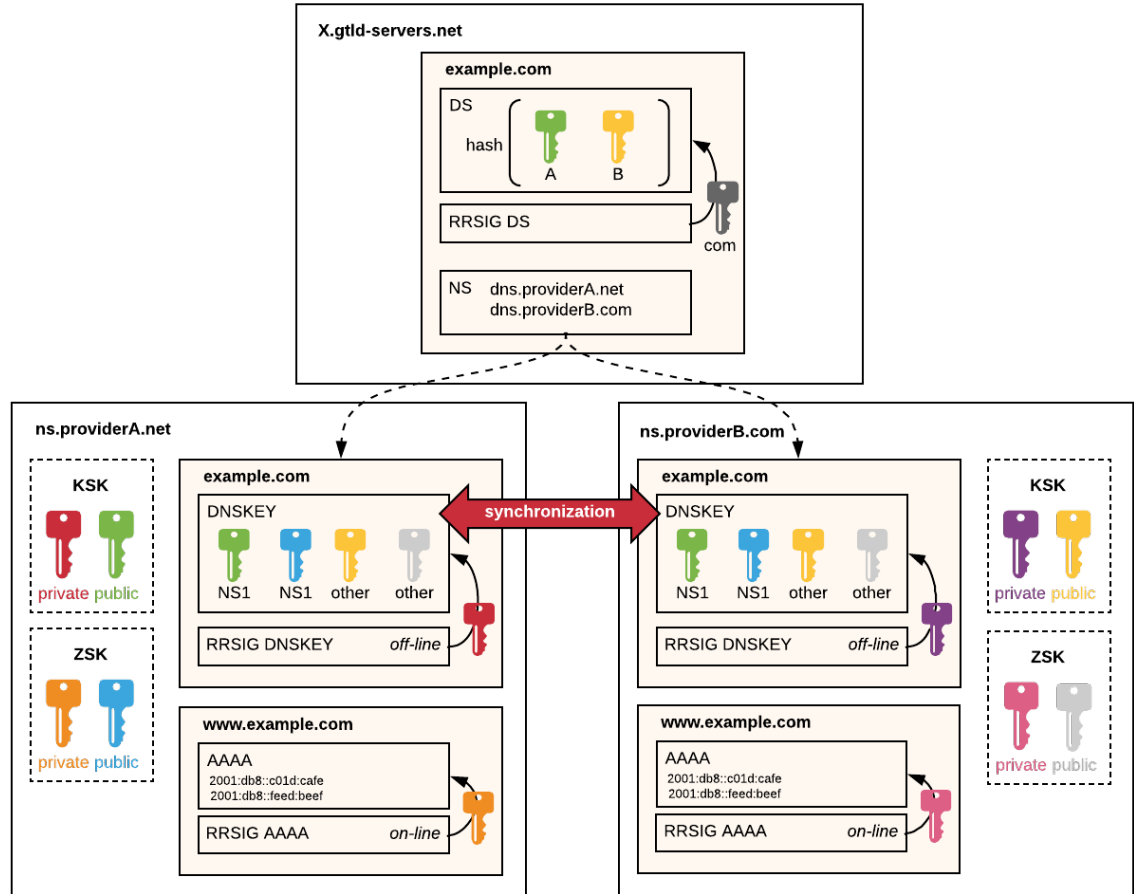
Hackathon Plan

- 2 type of project
 - Solving real operations issues
 - Multi-Vendor DNSSEC
 - CNAME at Parent/APEX
 - DNS Privacy
 - Oblivious DNS
 - DoH/DoT

Multi-provider DNSSEC

[draft-huque-dnsop-multi-provider-dnssec-03](#)

- **Multi-provider models** allow DNSSEC to be deployed across multiple DNS providers
- **Each independently signing the same zone.**
- This mode of operation is needed to accommodate configurations that deploy non-standardized features like traffic management.

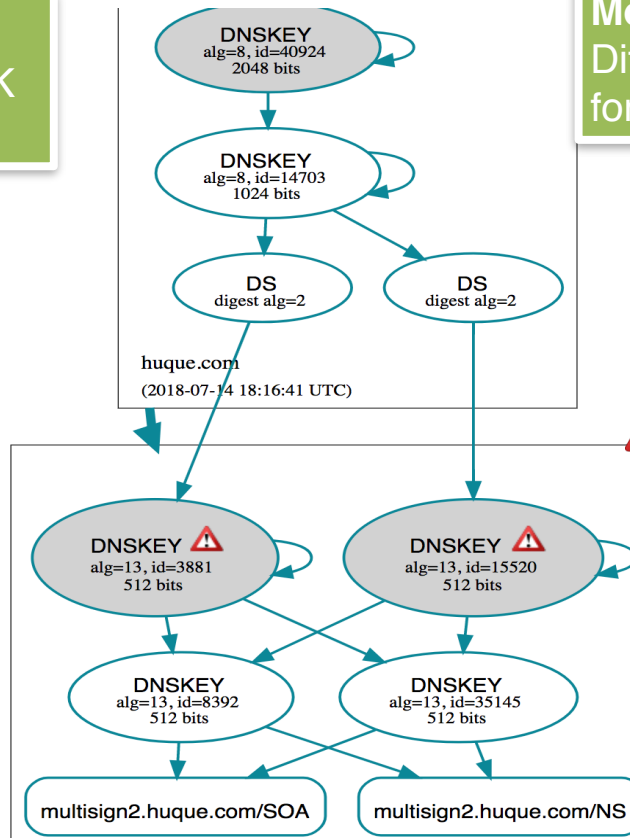
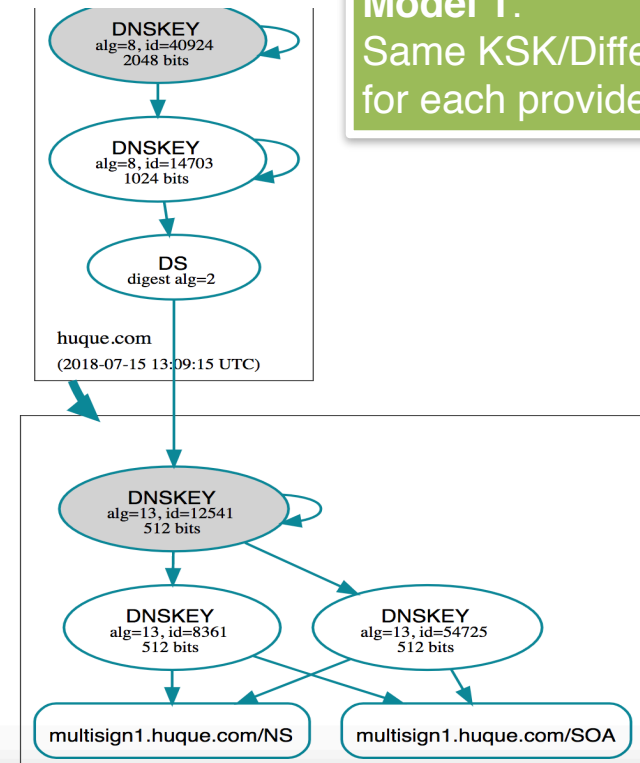


Multi-provider DNSSEC

[draft-huque-dnsop-multi-provider-dnssec-03](#)

Model 1:
Same KSK/Different ZSK
for each provider

Model 2:
Different KSK/ZSK
for each provider



Some DNS diagnostic tools flag this configuration even though validation works. These tools will likely need to be updated.

Accomplishments

- **Deployed and validated that both multi-provider models work**
- Noted that some **DNS diagnostic tools** issue warnings, because they didn't anticipate some configurations
- Drafted minimal **API for DNS providers** to synchronize ZSK public keys
- **Tools to check DNSKEY and DS RRsets** across servers for consistency

CNAME + DNAME draft

draft-sury-dnsop-cname-plus-dname/

1. Real Ops Issue: No (std) CNAME at Parent/Apex - we need a fix!!
 2. Put CNAME + DNAME in the parent zone & see what works/breaks
 3. Put CNAME + DNAME into the apex of the zone & see what works/breaks
- Setup:
 - Auth server: BIND 9.13.2 + experimental/cname-at-apex branch
 - Zones: cname-at-apex.rocks, cname-plus-dname.rocks

CNAME + DNAME draft

draft-sury-dnsop-cname-plus-dname/

1. Real Ops Issue: No (std) CNAME at Parent/Apex - we need a fix!!
 2. Put **CNAME + DNAME** in the parent zone & see what works/breaks
 3. Put **CNAME + DNAME** into the apex of the zone & see what works/breaks
- Setup:
 - Auth server: BIND 9.13.2 + experimental/cname-at-apex branch
 - Zones: cname-at-apex.rocks, cname-plus-dname.rocks



CNAME + DNAME draft

draft-sury-dnsop-cname-plus-dname/

1. Real Ops Issue: No (std) CNAME at Parent/Apex - we need a fix!!
 2. Put **CNAME + DNAME** in the parent zone & see what works/breaks
 3. Put **CNAME + DNAME** into the apex of the zone & see what works/breaks
- Setup:
 - Auth server: BIND 9.13.2 + experimental/cname-at-apex branch
 - Zones: cname-at-apex.rocks, cname-plus-dname.rocks



CNAME + DNAME @ PARENT

Results

DNSSEC Validation Enabled	No QNAME Minimization	Relaxed QNAME Minimization	Strict QNAME Minimization
BIND 9.11.4	OK!	N/A	N/A
BIND 9.12.2	OK!	N/A	N/A
BIND 9.13.2	OK!	OK!	OK!
PDNS Recursor 4.1.3	DNAME fails [2]	N/A	N/A
Unbound 1.7.3	OK!	OK!	OK!
Knot Resolver 2.4.0	N/A	Mixed [1]	N/A
Google Public DNS	OK!	N/A	N/A
Verisign Public DNS	OK!	N/A	N/A
Quad 9	DNAME fails [2]	N/A	N/A
Cloudflare 1.1.1.1	N/A	Mixed [1]	N/A

1. DNAME returns SERVFAIL *AND* Correct Resource Records
2. PowerDNS 4.2 has some DNAME fixes in the roadmap

CNAME at APEX

Results

DNSSEC Validation Enabled	No QNAME Minimization	Relaxed QNAME Minimization	Strict QNAME Minimization
BIND 9.11.4	CNAME MASKS APEX	N/A	N/A
BIND 9.12.2	CNAME MASKS APEX	N/A	N/A
BIND 9.13.2	CNAME MASKS APEX	CNAME MASKS APEX	CNAME MASKS APEX
PDNS Recursor 4.1.3	CNAME MASKS APEX	N/A	N/A
Unbound 1.7.3	CNAME MASKS APEX	CNAME MASKS APEX	CNAME MASKS APEX
Knot Resolver 2.4.0	N/A	CNAME MASKS APEX [1]	N/A
Google Public DNS	CNAME MASKS APEX [1]	N/A	N/A
Verisign Public DNS	CNAME MASKS APEX	N/A	N/A
Quad 9	CNAME MASKS APEX	N/A	N/A
Cloudflare 1.1.1.1	N/A	CNAME MASKS APEX [1]	N/A

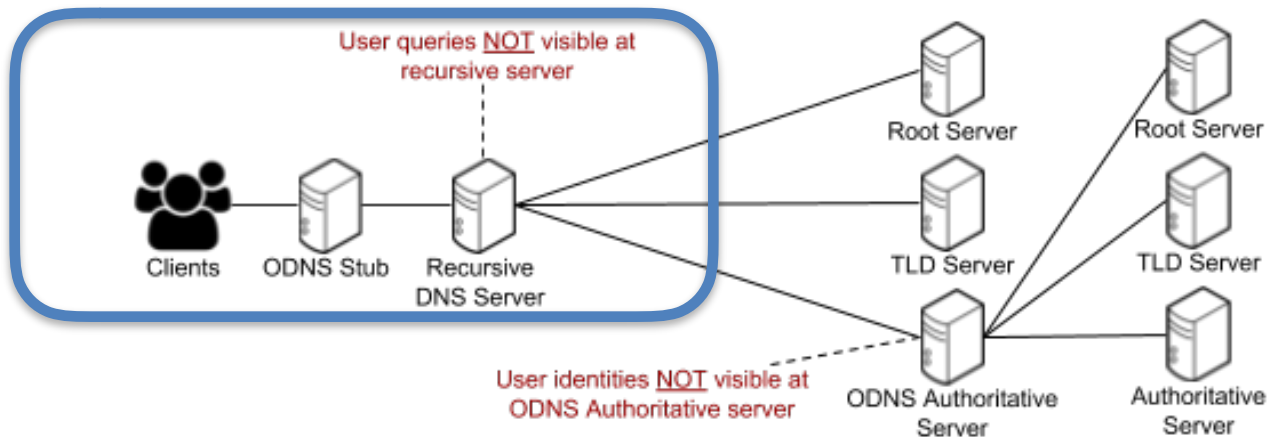
1. MX is masked to CNAME target, but SOA isn't

Nick Feamster
Willem Toorop
Ralph Dolmans
Allison Mankin

GOAL: No single entity
stub/recurse sees
both client IP + query
: add **ODNS stub**

Oblivious DNS

draft-annee-dprive-oblivious-dns/



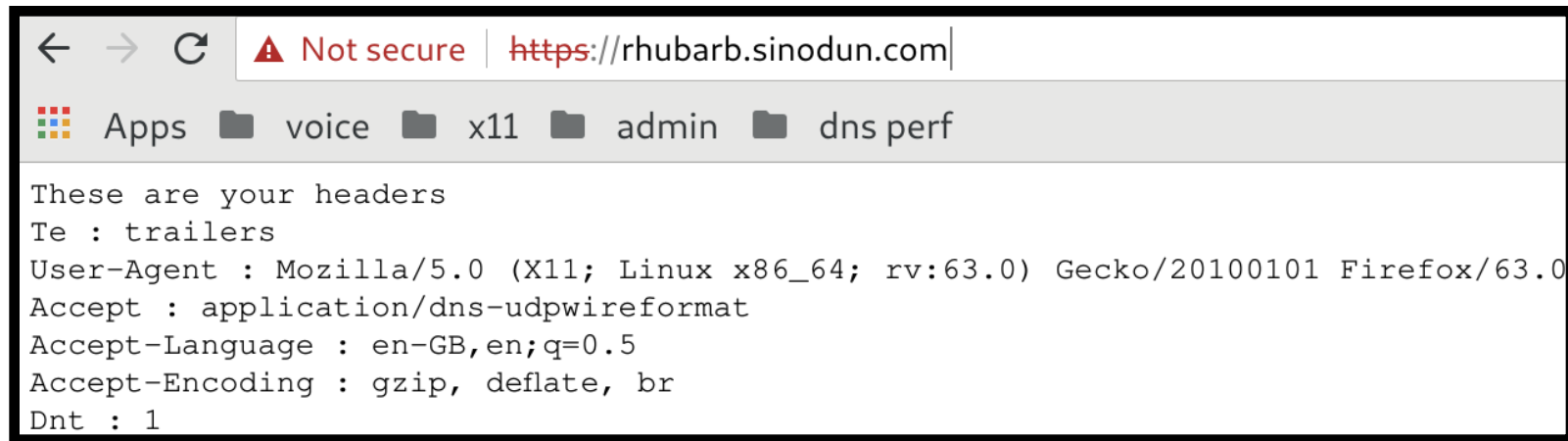
- Existing golang prototype: work started on porting to C (getdns/unbound)
- **DNS recommendations fed back to draft authors (and golang code)**
- Lots of new very cool (and short!) crypto implemented in C

DoH work

- **DoHPE**: Privacy/anonymity profile DoH (new draft)
- **DoH fingerprinting tool**
Proxies requests, displays headers (few lines of go)

Sara Dickinson,
Stephane Bortzmeyer, ++

John Dickinson

A screenshot of a web browser window. The address bar shows a red warning icon and the text "Not secure" followed by the URL "https://rhubarb.sinodun.com". Below the address bar is a tab bar with several tabs: "Apps", "voice", "x11", "admin", and "dns perf". The main content area of the browser displays the following text:

```
These are your headers
Te : trailers
User-Agent : Mozilla/5.0 (X11; Linux x86_64; rv:63.0) Gecko/20100101 Firefox/63.0
Accept : application/dns-udpwireformat
Accept-Language : en-GB,en;q=0.5
Accept-Encoding : gzip, deflate, br
Dnt : 1
```

Other projects

- **Recursive to Auth TLS:** [draft-bortzmeyer-dprive-resolver-to-auth/](#)

Port of old DNS-over-TLS patch to NSD trunk. Successful testing with kdig, getdns, etc. Some performance and corner case testing. No surprises...yet.

Stephane Bortzmeyer

- **DNS Zone Digest:** [draft-wessels-dns-zone-digest/](#)
Several updates will be reported to the authors

Shane Kerr

Wrap Up

Team members:

Stephane Bortzmeyer

Shane Kerr

Benno Overeinder

John Dickinson

Willem Toorop

Ralph Dolmans

Sara Dickinson

David Blacka

Shumon Huque

Jan Vcelak

Ondrey Sury

Allison Mankin

First timers @ IETF/Hackathon:

Vaughan Perry

Pallavi Aras