DNS-over-TCP/TLS Implementation

Sara Dickinson
Sinodun

DNSOP@IETF96 Berlin, July 2016

Recursive implementations

Features		Recursive resolver		
		Unbound	BIND	Knot Res
TCP/TLS Features	TCP fast open			
	Process pipelined queries			
	Provide OOOR			
	EDNS0 Keepalive			
TLS Features	TLS on port 853			
	Provide server certificate			
	EDNS0 Padding			

Dark Green: Latest stable release supports this
Light Green: Patch available
Yellow: Patch/work in progress, or requires building a patched dependency
Grey: Not applicable or not yet planned

Alternative server side solutions for TLS

- dnsdist would be great… but no support yet
- Pure TLS load balancer
  - NGINX, HAproxy,…
  - BIND article on using stunnel

But….
- server must still have full TCP capabilities
- pass through of edns-tcp-keepalive option
- DNS specific access control is missing

Stub implementations

Features		Stub					
		ldns (drill)	digit	getdns	BIND (dig)	Go DNS	Knot (kdig)
TCP/TLS Features	TCP fast open						
	Connection reuse						
	Pipelining of queries						
	Process OOOR						
	EDNS0 Keepalive						
TLS Features	TLS on port 853						
	Authentication of server						
	EDNS0 Padding						

- Dark Green: Latest stable release supports this
- Light Green: Patch available
- Yellow: Patch/work in progress, or requires building a patched dependancy
- Grey: Not applicable or not yet planned

DNS-over-TLS Deployment

- SERVERS: NLnet Labs and OARC offering experimental DNS-over-TLS servers:

https://portal.sinodun.com/wiki/display/TDNS/DNS-over-TLS+test+servers

- CLIENT: getdns - 1.1.0a1 release of a DNS-over-TLS daemon mode - try it out:

https://portal.sinodun.com/wiki/display/TDNS/DNS+Privacy+daemon

DNS-over-TLS services

- RIPE DNS WG: Presentation and discussion of offering experimental DNS Privacy Service
- RIPE are planning to co-ordinating a community effort
  - Research various solutions and issues
  - Output will be operational guidance

Ongoing Work

- Patches to dnsperf to do TCP/TLS performance benchmarking using RFC7766, etc.
- draft-ietf-dprive-dtls-and-tls-profiles-03
  - 2 updates since IETF 95 - please review!