Sara Dickinson <u>sara@sinodun.com</u>

DNS is evolving

DOT: DNS-over-TLS

DOH: <u>DNS-over-HTTPS</u> (WIP)

- DOT RFC7858 standard May 2016
- DOH draft <u>draft-ietf-doh-dns-over-https</u> is in WGLC
 - Deals with protocol, not detailed use cases or discovery
- Both are happening, both will change stub to recursor DNS in many ways.... focus on end user here

Implementation

	Client	Recursive Resolver
DOT	 getdns library Stubby (smart proxy) Unbound/Knot resolver (fwd) Android system config (dev) systemd (PR) Tenta browser 	 Unbound, Knot Resolver, dnsdist, CoreDNS, Tenta BIND on the way
DOH*	 Android 'Intra' App Firefox config option + "experiment" Stubby (next release) Various experimental 	Various experimental

^{* 10+} implementations (see DOH mailing list and IETF 101 Hackathon)

Recursive Resolver Deployment

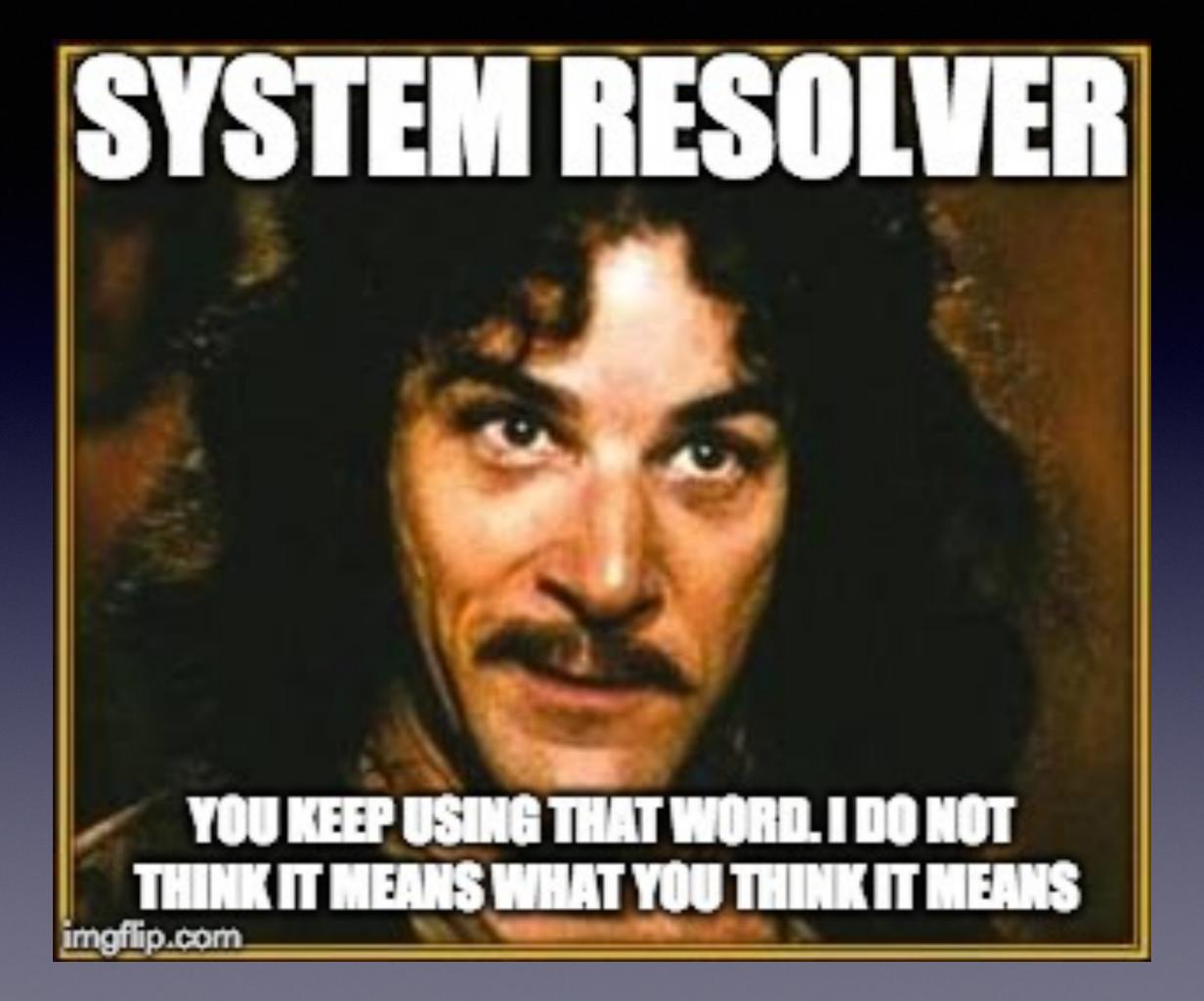
	Standalone	Large Scale
DOT	• <u>19 test servers</u>	• Quad9 (9.9.9.9)
		• Cloudflare (1.1.1.1)
DOH*	Google https://dns.google.com/experimental	Cloudflare https://cloudflare-dns.com/dns-query
	Few other test servers	

^{*} Experimental, some support JSON as well as wireformat

System or App?



- Always been technically possible for apps to do their own DNS, has just been the exception and not encrypted.
- getdns was designed as a modern, async DNS API with applications in mind (but also as a system wide component)
- DOH use case "allowing web applications to access DNS information via existing browser APIs"
 - Fully expect all browsers to offer DOH soon as browser wide option (will it ever be the default?)
 - Proposals about discovery of DOH server for a domain...



- In a 'cloud' based world, most queries go through the browser
- Other apps likely to follow and system component will use DOT/DOH
- But what does this practically mean for users?
 - Most won't notice...
 - Increased privacy (yeah!)
 - But.. complicates DNS management

- In a 'cloud' based world, most queries go through the browser
- Other apps likely to follow and system component will use DOT/DOH
- But what does this practically mean for users?
 - Most won't notice...
 - Increased privacy (yeah!)
 - But.. complicates DNS management



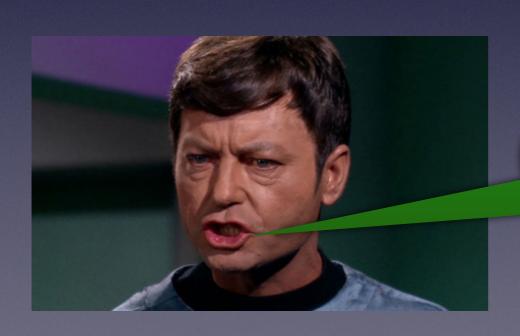
- Multiple config points (transport, authentication)
 - Importantly DNSSEC
- Multiple recursive resolvers
 - Scatter queries/reduce leakage
 - What if some fail, get blocking or attacked
- Multiple points for monitoring/debugging?
 - Will all apps expose DNS queries to users?
- Co-ordination of end device DNS is not obvious
 - System API to advertise user preferences?

- Multiple config points (transport, authentication)
 - Importantly DNSSEC
- Multiple recursive resolvers
 - Scatter queries/reduce leakage
 - What if some fail, get blocking or attacked
- Multiple points for monitoring/debugging?
 - Will all apps expose DNS queries to users?
- Co-ordination of end device DNS is not obvious
 - System API to advertise user preferences?

DNS no longer part of the infrastructure?

I'm not judging...
I'm just saying...

I'm not judging...
I'm just saying...



It's DNS Jim, but not as we know it

Thank you!