DNS WARS

A Presentation/Discussion

The St. Louis Unix Users Group

June 10, 2020

David Forrest

Bio

David Forrest graduated from Oregon State University in BA, Finance Emphasis, Physics & Mathematics. Lifelong hobbyist in IT from IBM 1401, Model 20, Model 30, Model 85, Sigma 7, XDS 7, SWTP 6800, M6809, 8080, 80286, 80386, OS2, and on to currently running XP, CentOS6/7/8, Raspbian, Mint, and Chrome on various local and cloud machines. My first was ALWAC-3G in 1962 running with 4K of rotating magnetic core memory.

Current Bio

I went to the grocery store and they now have a parking spot for Fat guys that like to grill. That's so considerate.

Dr. Paul Vixie

Presented the hour-long Keynote session at the Southern California Linux Users Expo SCaLE 18x in early March.

The Founder of ISC and still on its board.

Slides in black in this presentation are his; from:

https://www.youtube.com/watch?v=artLJOwToVY

Abstract

- Due to pervasive unpreparedness of users, applications, operating systems, and protocols, DNS has become an essential control point for “cyber” security. Most networks have a mix of legacy, modern, safe, and unsafe devices attached to them, and this condition won’t change as quickly as the Beyondcorp initiative might suggest. However, DNS is also an important control point for authoritarian regimes, and so “bypass” innovation is continuous, rapid, and ambitious. Special attention is deserved by the “DNS over HTTP” or “DoH” protocol now being strongly pushed by Mozilla, CloudFlare, and others. A brief mention will be made of IRTF Resolverless DNS.

DNS Wars – Earlier Episodes

- Ep. I: VeriSign™ and SiteFinder™ put a wildcard address at *.COM
  - Ending: delegation-only, delegation-only-except, lawsuit
- Ep. II: Anycast RDNS, OpenDNS, NXD redirection, Google redirection
  - Ending: creation of 8.8.8.8, with many others to follow
- Ep. III: Creation of EDNS Client Subnet (ECS)
  - Ending: less privacy+authenticity due to larger attack surface

DNS TODAY

The Domain Name System has been a critical enabler of Internet growth since its inception in 1987.

In the decades since then, the DNS resolution process has evolved from the LAN to the WAN, and to Anycast; it now includes DNSSEC validation, Extended DNS (EDNS) Client Subnet, larger message sizes, and I18N.

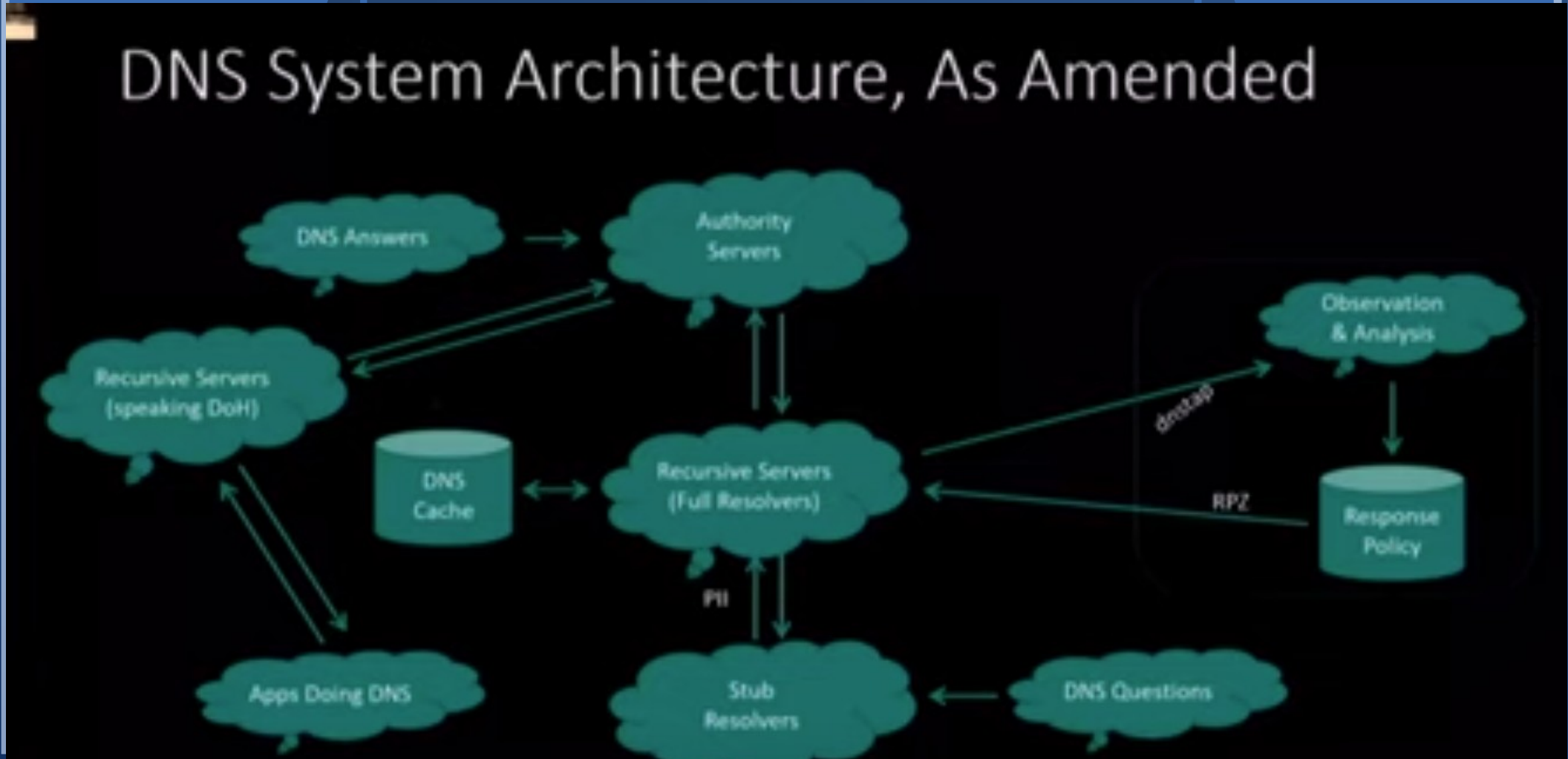
DNS RESOLUTION

The resolution process has also been abused for surveillance, advertising insertion, and exfiltration. Today the DNS resolution process is poorly understood, and yet under forced revision.

The trend is for DNS to be carried inside HTTPS where it cannot be monitored or controlled except by servers and clients themselves, and the dangers this will yield must be studied and discussed while the future remains flexible.

Internet System Topology, ~2019

DNS 2020


DNS System Architecture, As Amended
DNS Answers
Authority Servers
Recursive Servers (speaking DoH)
DNS Cache
Recursive Servers (Full Resolvers)
dnstap
Observation & Analysis
RPZ
Response Policy
PII
Apps Doing DNS
Stub Resolvers
DNS Questions

DNS Proposed

Now Under Construction: Resolverless DNS

- Web content providers and their CDN's want better performance
  - Which means, faster time-to-next-eyeball
- Most content includes many object references (images, scripts)
  - The time taken for a browser to look up these DNS names is measurable
  - (and may involve "ad blocking")
- Therefore an IRTF WG is studying "Resolverless DNS"
  - Here, DNS data will be "pushed" as part of a normal web content fetch
  - DNSSEC signatures won't be included; TLS is considered "secure enough"
- This terrifically broadens the attack surface of web site defacement
  - Bit coin mining JS can now be downloaded without triggering EP protections

Complexity

$$\left(\frac{n}{m+q}\right) < \frac{n}{m}$$

n is #/devices or #/technologies you use that you understand
m is #/devices or #/technologies you already have
q is #/devices or #/technologies you want to add

This fraction inversely predicts your complexity-related risk

So, What to do?

- Use Cloudflare et cetera and let them control access?
- Keep your own lists of crappy domains you want to exclude, understanding a third party may not have your pecularities?
- It is certainly easier to cede control.
- I decided to use dnsmasq to include an additional “prohibited” list that I’d control.

Cloudflare

- 1.1.1.1 for Families
- 1.1.1.1 for Families is the easiest way to add a layer of protection to your home network and protect it from malware and adult content. 1.1.1.1 for Families leverages Cloudflare’s global network to ensure that it is fast and secure around the world. And includes the same strong privacy guarantees that we committed to when we launched 1.1.1.1 two years ago.

- 1.1.1.1 for Families has two default options: one that blocks malware and the other that blocks malware and adult content. You choose which setting you want depending on which IP address you configure.

Cloudflare - continued

- Protect your home against Malware
- Using the following DNS resolvers will block malicioius content:
-
- 1.1.1.2
- 1.0.0.2
- 2606:4700:4700::1112
- 2606:4700:4700::1002

Cloudflare - 2

- Block Malware and Adult Content
- When you change your DNS resolvers to the addressess below, 1.1.1.1 for Families will block malware and adult content.
-
- 1.1.1.3
- 1.0.0.3
- 2606:4700:4700::1113
- 2606:4700:4700::1003
- Ready to set it up? You’ll find an easy guide for every device in the setup instructions page.

DNSMASQ

I use dnsmasq, refreshed nightly, with an additional /etc/hosts file for a maintained list of names to be blocked (assigned 127.0.0.1 & ::1)

[root@dave:~]# ll /etc/hostsipv6

-rw-r--r--. 1 root root 777K Jun 1 20:27 /etc/hostsipv6 (29,000 lines!)

[root@dave:~]# grep -v "^$\|^#" < /etc/dnsmasq.conf

- domain-needed
- resolv-file=/etc/resolv.conf.static (8.8.8.8;1.1.1.1)

  (my edge router assigns 192.168.1.73;8.8.8.8 for RDNS)
- domain=dave.maplepark.com
- conf-dir=/etc/dnsmasq.d,.rpmnew,.rpmsave,.rpmorig

But, still, uncertain am I

- Last week a concern expressed on the NANOG list about Cloudflare scared me a bit. Usbank.com was found unresponsive and determined that cloudflare had routing entries wrong. Yuck! That was my fallback.
- If we have time, I'll now show some details about my set-up. And answer any questions I can.
- And here are Dr. Vixie's end notes:

End Notes

- Every innovator solves the problems their/they customers have
  - Not every innovator knows or cares about systemic costs
- DNS is the first and only system of its kind that has scaled by 10^9
  - Distributed, coherent, reliable, autonomous, and hierarchical – unique!
- As in politics, economics, and climate change, this future is brutal
  - Our consent is no longer sought, and can only be withheld at notable cost
- Westphalian era is not strictly, completely, over
  - However, Space and I.T. operational domains ignore boundaries
  - "You can keep what you can defend" means something different vs. 1846
  - Some corporations now mostly have I.T. supremacy over most countries