Who Do I Trust?

Eric Ziegast, DomainTools LLC

DNS-OARC Day - Feb 26, 2024

History vs Response

- Goal: Reflect on events that created DNS technologies and changes in trust

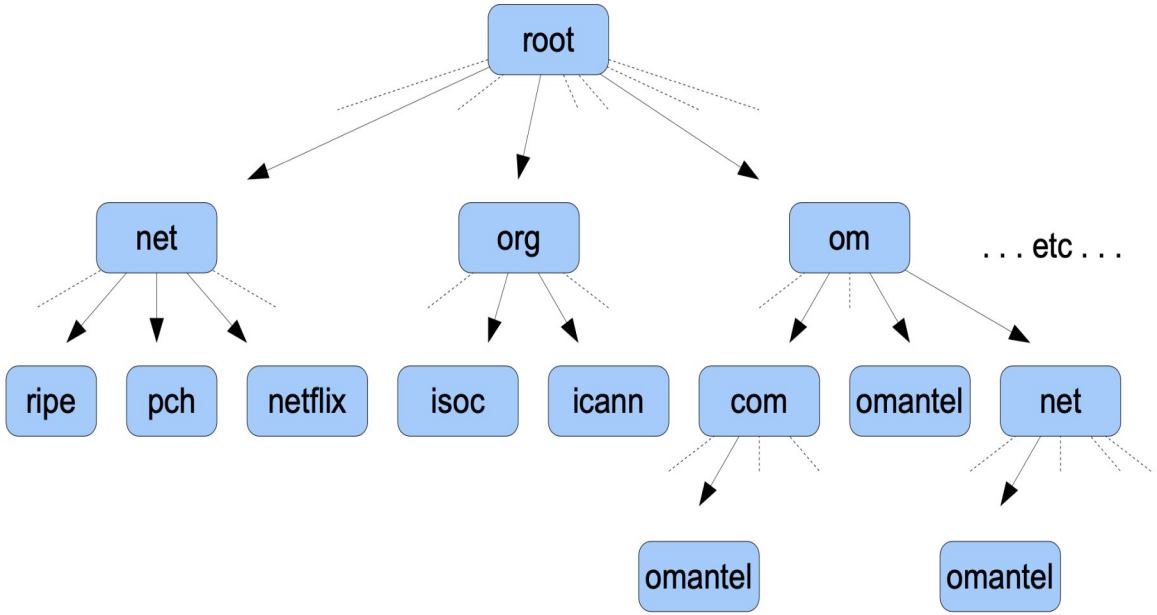
Inspired by:

Search: “DNS WARS Vixie NANOG Bypass”

Before We Needed To Scale

- Pre-DNS – not scalable (hosts.txt)
- Good Old Days (1990's)
  - BIND 4 (sparc, unix, bsdi, linux) or MS DNS Server
  - Specified Resolver or DHCP of a couple servers
    - Company IT Admin
    - University Network Team
    - Dialup provider or ISP provided via DHCP
    - Geeks ran their own recursive server
  - Non-commercial or included
  - No significant abuse – "Best Effort" – trustworthy operators

“The DNS” - Heirarchical



InterNIC
- SRI
- Network Solutions

ICANN
- US Entity… hmmm
- Now multi-stakeholder

Trusted? Yes? No?

ccTLD vs gTLD policy

Registrars vs Registries

“The” DNS?

- Anyone remember AlterNIC (1995)? link
  - “The DNS” was not sufficient
  - Original sin - DNS Cache Poisoning (glue)

Even today:

- OpenNIC - link
- .Onion – TOR link
- Blockchain / Decentralized- link

Meanwhile – software diversity emerges

- Trust the software?
  - Bundled with most operating systems – but no direct support
  - BIND known for CVEs – remote exploit - overflow
  - Where does nameserver belong in infrastructure? (“the event”)
- djbdns
  - Distrust in BIND and ISC in general
  - Separate Recursive from Authoritative
  - Alternative implementation (but avoided DNSSEC)
- Nominum – commercial focus for larger operators – rewrite
- Microsoft makes own interpretation on HESIOD (loose vs strict)

DNSSEC

- Anti cache-poisoning cryptographic technology
  - Heirarchical trust like DNS
  - New complexity – sometimes failure - oops moments - dnsviz
- “The DNS” has a root
  Key signing ceremony
  Trust in seven people - link
- Chicken and Egg – Scaling adoption – “DLV” - trust
- Now that we have DNSSEC – How about DANE? No?
  - Trust SSL? Really?

Another cache poisoning threat

- “Kaminsky attack” - WIRED article
- DNSSEC more important than ever, but not universally adopted
- New trust and cooperation model on responsible disclosure tested
- “Trust groups”

  Lesson: Prior planning and preparation needed for next event – PGP too

Monitoring

- DNS is two protocols – below and above recursive server
  - “RD=1” Device asks the recursive resolver (UDP or TCP in the clear) for an answer. Source client IP address/port is visible. Discover which sources tried to access known malicious domains.
  - “RD=0” Recursive resolver asks authoritative servers for information. Basis of PassiveDNS replication. PII-free monitoring of “The DNS” very useful for security researchers – map of the DNS.
- Network administrators have a role to protect their network and its users. They can access network data, including DNS data from the network.
- Not a problem until operators perceived losing trust.

Public Recursive Servers

- OpenDNS (2006)
  - Better service – anycast, large cache, reliable
  - Features – like filtering, analytics, and alternative answer for Google
- Google 8.8.8.8 – reaction
  - No logging accessible to third parties – unaltered and unfiltered results
  - Extensive presence/infrastructure
  - Very easy to remember - widely adopted as alternative to DHCP
- Cloudflare and Quad9
  - Privacy-centric – some filtering
- Other servers – Country specific

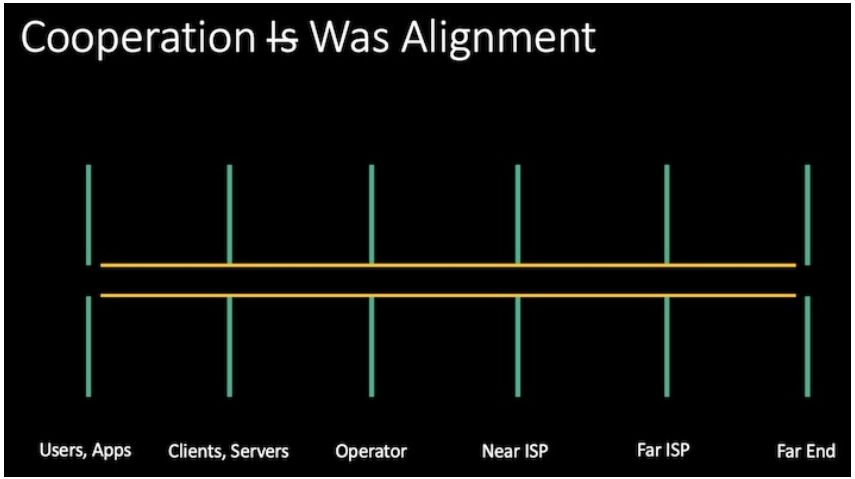
DNS4EU

- Reaction to quads
  - none of quads are Europe-centric
  - GDPR
  - European regulations for filtering
- RIPE’s opinion slightly different
  - Diversity needed to prevent monoculture
  - Guidelines (link)

IT Manager: What is your VPN policy?

- DoT/DoH offered – great for privacy, but can be used maliciously
- There are some “opt-out” domain hooks (useful for IT environment)
- Some like Firefox/CloudFlare or Apple/Cloudflare turn on DoH by default.
- If you don’t want tunneling of C&C via encrypted DNS, need to offer your own servers, possibly prevent external tunnels.

.

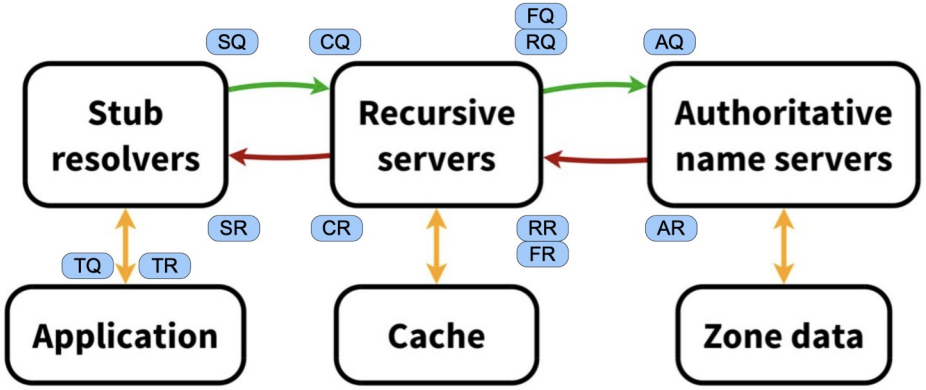


IT Manager or ISP

- Can you do a better job than outsourcing?
  - Appliance vendors / Private Resolver as a Service / Public Recursors
  - Redundancy/uptime?
  - Do you have data you need to protect?
  - Does your view of Internet need to differ from “The DNS”?
- Are you prepared to monitor servers and respond to issues?

Monitoring

- As encryption deployed between clients and servers, network monitoring becomes less useful
- DNSTAP! (link)
- High performance binary logging built into mainstream resolvers
- CLIENT_QUERY
  - Below recursor, PII
- RESOLVER_RESPONSE
  - Above recursor, PassiveDNS



DNSmonster

- You want to collect data and feed it into your existing security operations
- Integrations with several visualizations and data management tools (like ClickHouse or Elastisearch).
- dnsmonster.dev

pDNSSOC

- An engine for integrating threat indicators with DNS monitoring
- Create a “Poor man’s SOC” with less effort – open source too
- Utilizes DNSTAP for monitoring
- Malware Incident Sharing Platform (MISP link)
  - Widely used in TI and CSIRT communities
- pDNSSOC in github
- Presentation video

While you're logging

… PassiveDNS plug ...

- The internet security industry needs anonymized response data
- Large operators consolidating DNS resolution silo it - benefit/risk
- Organizations I work with do our best to look after privacy of contributors' clients.
- Enhance regional representation of data that help detect threats

Speaking of filtering

- Registries/registrars cannot efficiently take down malicious domains.
  - Fast weaponization of malware
  - Lack of trust in reporters
- Response Policy Zones ecosystem – “DNS firewall”
  - Block or wall-garden based on names, IPs, nameservers
  - Breaks DNSSEC promise – a below-recursor override
- My server(s), my rules!
- What content needs to be filtered? What jurisdiction? Trust issue

DNSRPZ

- Efficient, scalable – add/remove/distribute entries via IXFR
- Private distribution – TSIG
  sidebar - learned from DNSBL experience
- Use public lists available from threat intel providers
- Create your own, including “whitelists”.

Trust in the DNS?

- It is becoming too complicated to implement everything in DNS without the potential for something new breaking something. (eg: DELEG)
- Be strict in what you send and flexible in what you accept.
- Not all software implements the same way – unexpected behavior.
- Debugging gets more difficult for everyone.

DNS Camel

Herding the DNS Camel

Bert Hubert

21 Nov 2018

Bert Hubert, the founder of PowerDNS and author of RFC 5452, shares his views on forces influencing DNS protocol development.

Do app developers trust DNS?

- Check our Geoff Huston’s talk tomorrow
- If application developers have difficulty in how their clients utilize DNS to interact with their server infrastructure, what can application developers do?

Good News

- DNS-OARC is a vibrant community
- All the best researchers and software implementors attend in some form
- DNS-OARC makes data available and supports analysis tools to help operators see changes or confirm hypothesis about events

- Use this opportunity to meet and build relationships

Great example

- OARC 42 - Tudoor attack
  - https://www.youtube.com/watch?v=4fjhfPzu01M

My Observation:

- ICANN – people care about reducing business friction for the DNS
- IETF – people want new things implemented the way their organization wants
- DNS-OARC – people care that the DNS can keep working

How about you?

- How are you navigating changes in how clients are accessing DNS and Infrastructure in general?
- Are you planning changes in how your constituency uses the DNS?