USC/ISI's TLS at a Root Experiment

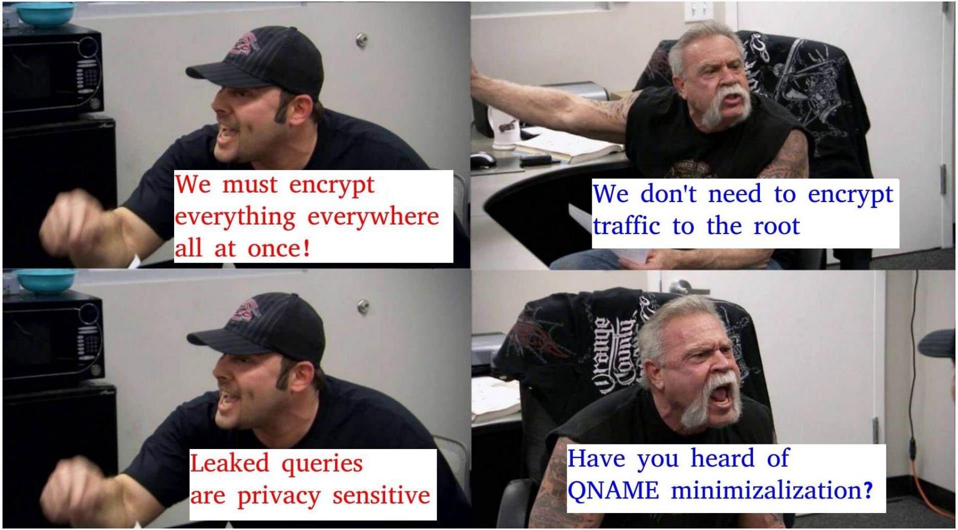
episode 2 – the saga continues

Wes Hardaker

2023-02-24

Should DNS over TLS be deployed at the root?

There is general disagreement. . .

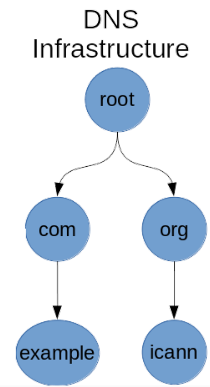

We must encrypt everything everywhere all at once!
We don't need to encrypt traffic to the root
Leaked queries are privacy sensitive
Have you heard of QNAME minimizalization?

... about TLS deployment at the root

That doesn't protect keyword searches
Then deploy NSEC agressive caching!!
That still leaks! I'm deploying TLS at b.root-servers.net
Fine! Then kiss your CPUs goodbye!

The Outstanding Questions

- Should DNS over TLS be deployed to all servers?
  - at resolvers?
  - at registrant's servers?
  - at TLDs?
  - at the root?
- Can you help answer these questions?



TLS at the root today

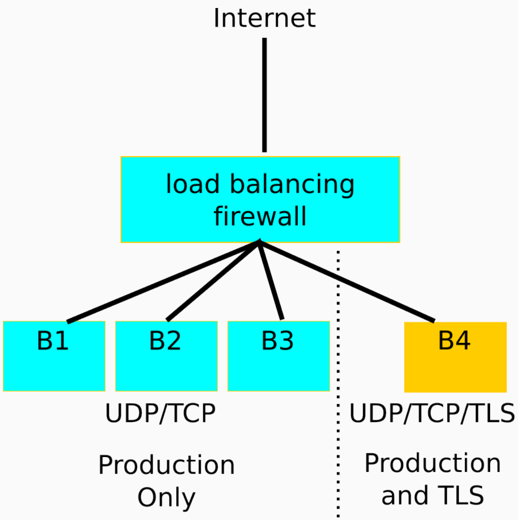
- In 2019 (ish) USC/ISI started discussing future TLS at b.root-servers.org
- In 2022/07 Google and USC/ISI conducted an early TLS experiment at B @ SIN
  - Defined a safe and isolated architecture for testing TLS
  - Experiment deemed a success
  - Reported collected metrics at DNS-OARC

TLS at the root today

- In 2019 (ish) USC/ISI started discussing future TLS at b.root-servers.org
- In 2022/07 Google and USC/ISI conducted an early TLS experiment at B @ SIN
    - Defined a safe and isolated architecture for testing TLS
    - Experiment deemed a success
    - Reported collected metrics at DNS-OARC
- Now it's time to involve you!
    - TLS deployed to all b.root-servers.org
    - Open for experimentation

Isolation Architecture

- Firewall's role:
  - Isolate normal production from TLS traffic
  - Filtered by port (853)
- Most CPUs handle only regular DNS traffic
  - One dedicated to support both TLS and regular traffic



TLS at the Root

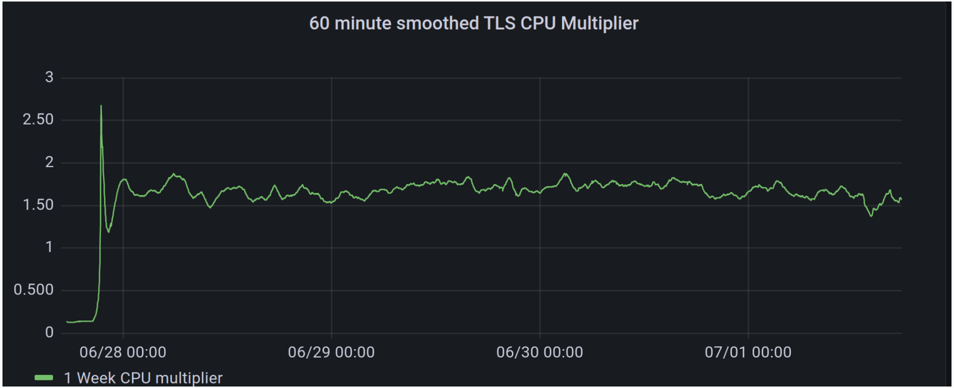
Research for Everyone Everywhere

Some questions we want to answer

- Can this be done safely?
    - *in parallel with critical infrastructure*
- Can this be done at scale?
- What metrics should we collect?
    - *traffic levels, CPU load, memory, etc. . .*
- How do we report these metrics?
- How do we continue to support DITL collection?
- If we build it, will they come?

Example past metrics we've reported on

- CPU overhead of TLS



What questions can you pose?

- Is TLS at the root helpful?
- How will you perform service discovery?
- How will you probe authoritative servers for TLS support?
- How will you handle partial authoritative support?
  - E.G., b.root-servers.net is the only root server with TLS
- ??? your idea here ???

Let's begin together

- Let's find out who's right
- Bring your own experiments
- We want to hear from you
- reach out: *b-poc@isi.edu*