# Enabling testing of TLS at the root

Wes Hardaker
hardaker@isi.edu
USC/ISI

January 17, 2023

It has been a recent standing question about how to deploy DNS over TLS on the authoritative side of the DNS infrastructure. Some proponents believe it will be challenging, and other challengers think that it will never be needed or deployed at the root. A famous "scientist on TV" one proclaimed:

> Yeah, but your scientists were so preoccupied with whether or not they could, they didn't stop to think if they should.
>
> – Dr. Ian Malcolm

At USC/ISI's root server we have recently studied the question of *"what impact would deploying TLS at the root to our root name server instances?"*. To answer this we agreed on an experiment with Google to separate out their queries from the rest of the queries arriving at our Signapore DNS Root instance. We then measured the traffic and load levels at our instance from all google IP prefixes, and again in the following week once we enabled TLS. The results show increases in packet counts, bandwidth and CPU overhead were presented at DNS-OARC [1] and partially summarized in Table 1. We also described how we could safely divide our architecture to safely enable this experiment.

| **Measurement** | **Multiplier** |
|---|---|
| PPS RX | 2.12 |
| PPS TX | 1.54 |
| Bandwidth RX | 1.90 |
| Bandwidth TX | 1.60 |
| CPU Load | 1.60 |

Table 1: Resource increase measurements from deploying TLS at the root

Having deemed this experiment a successful effort, we now announce that TLS support at *b.root-servers.net* is now available for general use and testing. We next want to hear from researchers and experimenters how and if you will use this new service, with the caveat that it is currently deemed a research experiment and is not guaranteed to be a permanently enabled service. Yet. Your opinion and results will greatly factor into whether or not we enable this as a permanent service.

## References

[1] Wes Hardaker. Tls at a root experiment. Talk at DNS-OARC, 07 2022.