T-DNS: Connection-Oriented DNS to Improve Privacy and Security

IETF 89 DNSOP

USC/ISI
John Heideman
Zi Hu
Liang Zhu

Verisign Labs
Allison Mankin
Duane Wessels

Why Consider T-DNS

- Privacy – Lacking encryption, vanilla DNS is susceptible to eavesdropping; especially so given widespread use of WiFi and third-party recursive DNS services.
- Spoofing – UDP's connectionless nature makes it ideal for use in reflection/amplification attacks.
- Fragmentation – Large DNS responses are increasingly common, leading to IP fragmentation and a new set of security concerns.

Proposed: New EDNS0 bit “TO”

a.k.a. STARTTLS for DNS

1. Establish TCP connection.
2. Client sends (dummy) query with TO bit set.

   “Hey, let’s upgrade this connection to TLS!”
3. Server responds with TO bit set.

   “Yeah, I’m down with that!”
4. TLS session negotiation commences.

Dummy Query

- Draft recommends:
  - query: STARTTLS/CH/TXT
  - response: an informative message
- Also innocuous:
  - query: ./IN/NS or ./IN/SOA
  - response: as appropriate

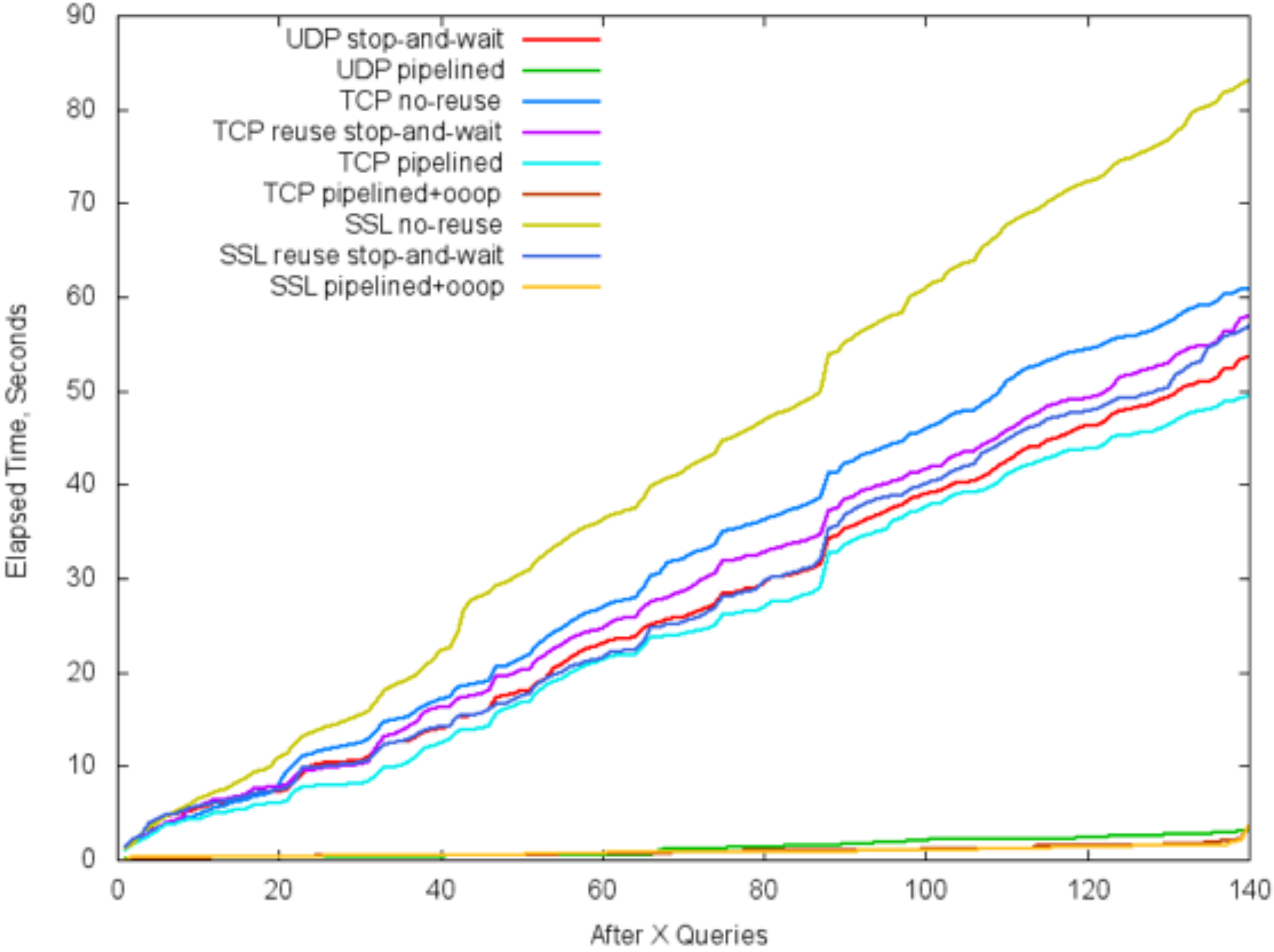
Sending TO over UDP

- Even though UDP can’t be upgraded to TLS…
- Client can include TLS-capable server knowledge in its server-selection algorithm.
- Servers can track deployment of DNS/TLS over time (see DO bit).
- For Discussion: what if middleboxes just drop a UDP query with this mysterious TO bit?

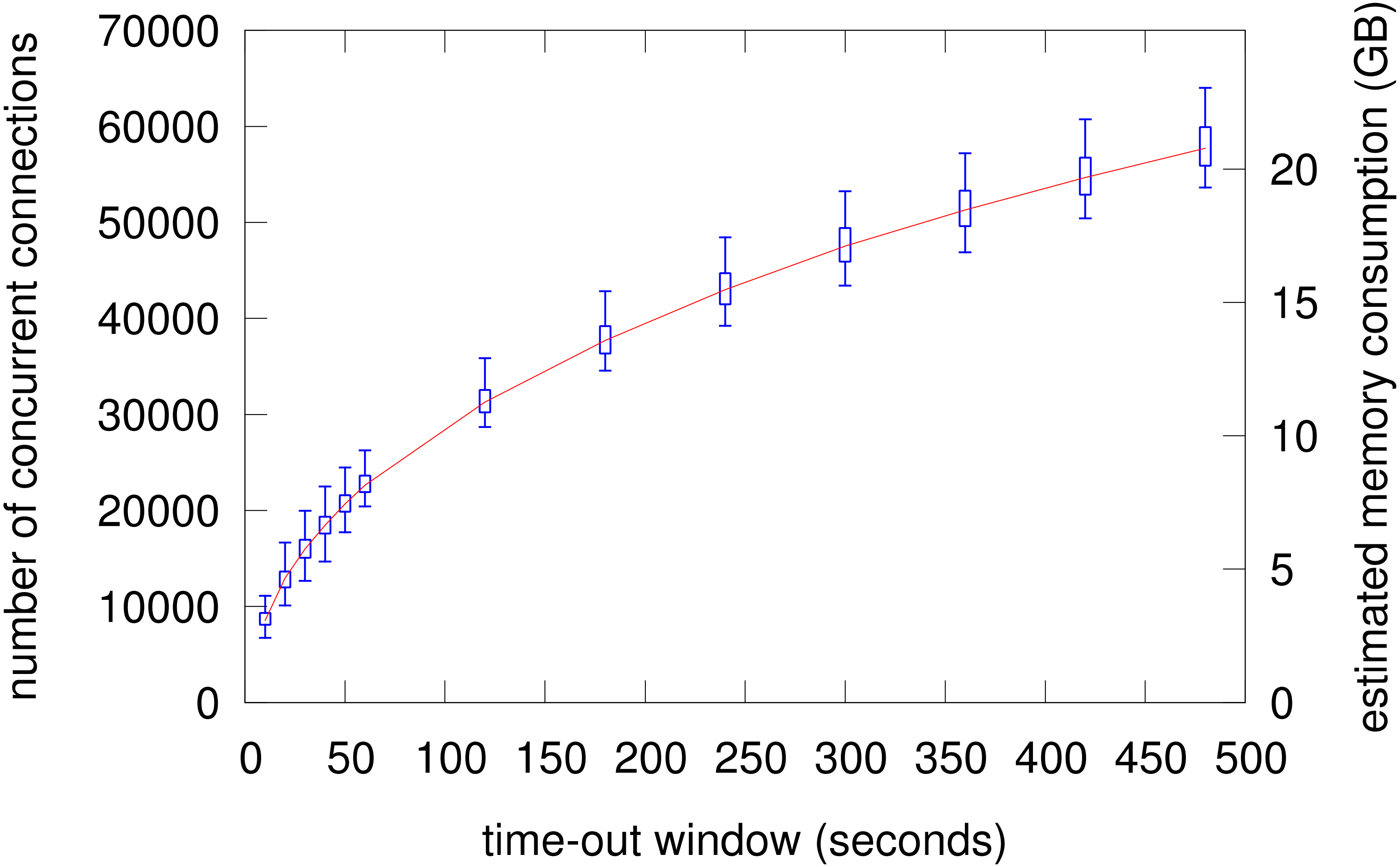
TO bit not protected

- For discussion: An adversary can prevent TLS upgrade by always blocking/stripping TO bit.
- Out-of-band method to know a server should accept TLS?
- Use a separate port number?

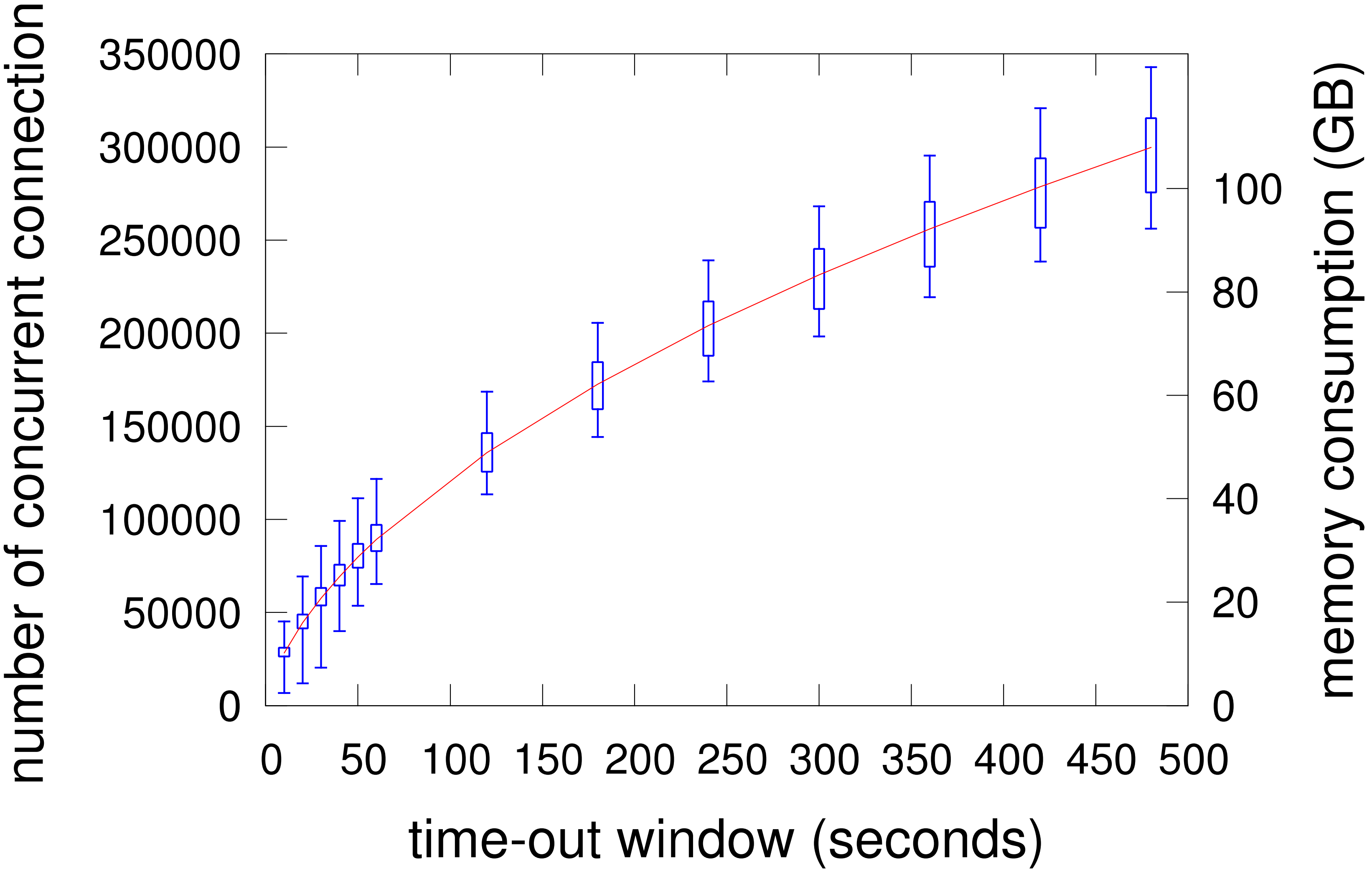
Latency Measurements
How long to send 140 queries?



Simulated Connection Reuse
stub-to-recursive



Simulated Connection Reuse
recursive-to-authoritative



Further Information

- draft-hzhwm-start-tls-for-dns-00
- T-DNS: Connection-Oriented DNS to Improve Privacy and Security
  - ftp://ftp.isi.edu/isi-pubs/tr-688abs.htm
- http://www.isi.edu/ant/tdns/index.html