Measuring the Global Reachability of DNS over TLS

Nick Feamster, *Princeton University*
Allison Mankin*, Salesforce*

Unencrypted DNS queries are vulnerable to eavesdropping attacks; additionally, an increasing number of network-connected devices in the Internet of Things (IoT) may leak sensitive or private information over unencrypted DNS channels [1]. To address these and other privacy concerns, recent standardization efforts have defined a mechanism to exchange DNS queries and responses over an encrypted TLS channel on a well-known port, 853 [2]. In light of this effort, we aim to study the reachability of port 853 traffic from as many vantage points on the Internet as possible, in an attempt to uncover characteristics of regions and networks where port 853 is consistently unreachable.

To perform these measurements, we rely on a tool that we have previously developed, Encore [3][4], which collects reachability measurements from web clients using cross-origin requests. A web client who visits any of the approximately 15 websites where Encore is installed is induced to perform a cross-origin request to a URL that is under our control, in this case, to a temporary site at the hostname porttest.verisignlabs.com. Using this mechanism, we can test whether these web clients can successfully reach URLs at standard ports (e.g., 80, 443), as well as the newly proposed port for DNS over TLS (port 853).

Over the course of approximately six months, we collected about 50,000 reachability measurements from 123 countries. This data set is relatively small,but its wide geographic dispersal points to issues for global access to eavesdropping-resistant DNS. Our preliminary results indicate that at least 5% of requests to port 853 are failing, and that these failures may be occurring disproportionately in certain geographic regions. We will also report on counterfactual analysis (in progress now) to determine whether these failures are systemic across all of the ports we are testing or specific to port 853.

Acknowledgement: Duane Wessels of Verisign, a co-author of RFC 7858, provisioned and operated the test server for the measurements.

[1] Nick Feamster. “Who Will Secure the Internet of Things?”, January 2016. https://freedom-to-tinker.com/blog/feamster/who-will-secure-the-internet-of-things/
[2] Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels, P. Hoffman. “Specification of DNS over TLS.” , RFC 7858, May 2016. https://tools.ietf.org/html/rfc7858
[3] Encore. https://encore.noise.gatech.edu/
[4] B. Jones, R. Ensafi, N. Feamster, V. Paxson,N. Weaver. “Ethical Concerns for Censorship Measurement.” SIGCOMM Workshop on Ethics in Networked Systems Research, August 2015. https://www.cs.princeton.edu/~bj6/papers/ns-ethics2015-censored-planet.pdf