GR-151 Performance Analysis and Review of Encrypted DNS Protocols

INTRO/ABSTRACT

Data encryption has quickly become an essential service of the internet. When it was first developed, data encryption and privacy were not prioritized. However, as the internet has grown and globalized, ensuring data privacy has become a prevailing requirement for conducting all types of business over the internet. Since privacy was an afterthought in the early development of the internet, many technologies have been built on top of existing ones in order to rectify security holes inherent in design. One of the more recent areas where this is happening is Domain Name Resolution. There are now competing mechanisms for encrypting DNS. I plan to explore two of the most common, DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT).

METHODS

To perform my analysis, I setup a virtual private server with the Ubuntu operating system and installed the Adguard Home DNS server. This allowed me to use DoT and DoH, freely switching between both (or neither) for testing. I then used the DNS Benchmark utility to resolve the top 50 websites using Adguard Home's upstream servers for each protocol. I also tested client-side encryption for each protocol using ten domains of my choosing.

RESULTS

Results showed that encrypting DNS requests did produce a performance impact on DNS resolution. DNS Benchmark showed that DoT and DoH were 15% and 20% slower respective to plain text requests. Additional tests showed they were 36% and 65% slower when encryption was performed by the client.

A performance analysis of DNS-over-TLS and DNS-over-HTTPS using public upstream DNS resolvers as well as client-side DNS encryption.

KENNESAW STATE UNIVERSITY
COLLEGE OF COMPUTING AND SOFTWARE ENGINEERING

Author: Jon Matthew Williamson
Advisor: Ahyoung Lee