On the Efficacy of DNS Resolver Privacy Preservation

Gene Tsudik and Christopher A. Wood

University of California Irvine, Irvine CA, USA
{gene.tsudik,woodc1@}uci.edu

Abstract. TODO

1 Introduction

The need for a private Domain Name System (DNS) has become increasingly important in recent years. There are currently several different proposals to address this growing problem, including DNS-over-TLS [**?**] and DNSCurve [**?**]. The former approach enables clients to create ephemeral sessions with either their resolver or authoritative (stub) servers in which queries can be issued. The latter uses per-query encryption to protect queries between clients and servers. Encryption is core mechanism used to enable client privacy in both of these solutions. However, in a recent study, Shulman showed that the privacy properties of these solutions (based on encryption alone) against eavesdropping adversaries [**?**]. This assessment showed that information leaked in DNS side channels, e.g., query timing, frequency, and resolution "chains," may reveal the target domain for a given DNS query. Moreover, by observing the trust properties of DNS servers and their responses, an adversary may also learn the specific record within a domain that was requested.

In this work we study a complementary problem. Namely, how can DNS queries, encrypted or not, be used to identify their clients? Put another way, do the contents of queries recursively issued by resolvers reveal information about the resolver's clients? This is an important problem because if answered positively, then stub servers can learn information about DNS clients even if encryption (without mutual authentication) is used to protect the actual contents of queries in transit.

The rest of this report is organized as follows. In Section **??** we formalize the adversarial model and XXX

2 System Model

The DNS system is composed of clients C, recursive resolvers R, and stub (authoritative) servers S. In the simplest use case, clients want to map a domain name to an IP address to establish a connection with a web server or host. Clients express queries to a recursive resolver that is responsible for finding the answer to this mapping query. If the answer to the query has not yet been fetched and previously cached, then the recursive resolver proceeds to ask the question to stub servers, starting at the root for the top-level-domain (TLD). For example, if the client query is `a.b.com`, then the stub associated with the com TLD is queried for the answer. Among the possible options, the

stub may return either an address (in an A record) or a pointer to another stub server to query (in a NS record). The resolver will recursively query stub servers until (a) an address is returned or (b) a "non-existent" flag indicating that the name cannot be resolved to an address. This final result is then relayed to the client to complete the process.

The DNS standard