ANÁLISE DO DESEMPENHO DE PROTOCOLOS PARA PRIVACIDADE NO DNS[1]

Guilherme Roberto Utech[2], Rafael Rodrigues Obelheiro[3].

[1] Análise do desempenho de protocolos para privacidade no DNS"
[2] Acadêmico (a) do Curso de Ciência da Computação – CCT – Bolsista PROBIC
[3] Orientador, Departamento de Ciência da Computação – CCT – rafael.obelheiro@udesc.br

Um requisito básico de praticamente toda aplicação Internet é mapear nomes de domínio em endereços IP. Esse mapeamento é realizado pelo DNS (Domain Name System). O objetivo deste mapeamento é fazer a conversão de um domínio amigável ao humano a um endereço amigável para a máquina. O protocolo DNS pode usar tanto UDP (User Datagram Protocol) quanto TCP (Transmission Control Protocol) como protocolo de transporte. Para minimizar a latência e a carga sobre os servidores DNS, tipicamente é usado o UDP, que não exige o estabelecimento de conexão. Tradicionalmente as transações DNS não são cifradas, o que significa que não é empregado nenhum mecanismo para garantir a confidencialidade do tráfego, o que permite a vinculação entre usuários e seu tráfego DNS, o que pode ter consequências importantes sobre a privacidade desses usuários. Saber quais nomes são consultados por um usuário pode ser usado para fins de marketing, para traçar um perfil de quais são seus interesses e preferências, e até mesmo determinar com quem ele se comunica. Neste trabalho será apresentada uma análise no desempenho de protocolos de privacidade para o DNS que provém privacidade através da cifragem do conteúdo.

Este trabalho de pesquisa tem como objetivo estudar a utilização dos protocolos que provém privacidade ao DNS realizando uma análise comparativa do seu desempenho utilizando métricas como latência. Os protocolos utilizados neste trabalho foram:

- DNS over TLS (RFC 7858): Provê confidencialidade e integridade de mensagens DNS usando Transport Layer Security (TLS) sobre TCP como transporte.
- DNS over HTTPS (RFC 84848): Provê confidencialidade e integridade de mensagens DNS usando HTTP sobre TLS e TCP como transporte.
- DNS over QUIC (draft-ietf-dprive-dnsoquic-03): Provê confidencialidade e integridade de mensagens DNS usando QUIC sobre UDP como transporte.

Este estudo é uma pesquisa aplicada na qual os principais métodos utilizados foram o estudo de caso e a revisão bibliográfica. O estudo iniciou-se com a revisão bibliográfica buscando expandir o conhecimento sobre ataques à privacidade no DNS e os protocolos DNS, DNS over QUIC, DNS over HTTPS, DNS over TLS, entre outros. Após isso iniciou-se uma fase de definição de métricas a serem utilizadas e ferramentas a serem utilizadas no experimento. Em sequência iniciou-se o planejamento dos experimentos e posteriormente a isso, iniciou-se os experimentos e a coleta de dados. Por fim foi realizada a análise dos dados coletados e a escrita do relatório.

A Figura 1 mostra os resultados obtidos pelos experimentos trazendo uma comparação da latência observada por cada protocolo variando o tamanho da resposta. Para realizar consultas com tamanho de respostas pré-definidas foi configurado uma zona DNS com registros TXT que produzem respostas com os seguintes tamanhos:

- p.dnstest: 100 bytes
- m.dnstest: 500 bytes
- g.dnstest: 2000 bytes

Apoio: CNPq Conselho Nacional de Desenvolvimento Científico e Tecnológico; fapesc Fundação de Amparo à Pesquisa e Inovação do Estado de Santa Catarina; GOVERNO DE SANTA CATARINA

- xg.dnstest: 4000 bytes

Nota-se que o protocolo DNS over QUIC (DoQ) apresenta um desempenho inferior em relação às outras propostas, e apresenta um aumento da latência conforme o aumento do tamanho das respostas. As outras propostas apresentam um desempenho equivalente e não apresentam variação notável de aumento de latência com o aumento do tamanho de resposta. O protocolo DNS over QUIC (DoQ) também apresenta uma grande variabilidade das respostas em comparação com as outras propostas.

Com isso, pode-se concluir que dentre as propostas observadas o DNS over QUIC (DoQ) é a proposta que apresenta o pior desempenho. Na continuidade da pesquisa, pretende-se ampliar a coleta de dados, aprofundar a investigação nos protocolos de privacidade no DNS e melhorar a infraestrutura de coleta de dados.

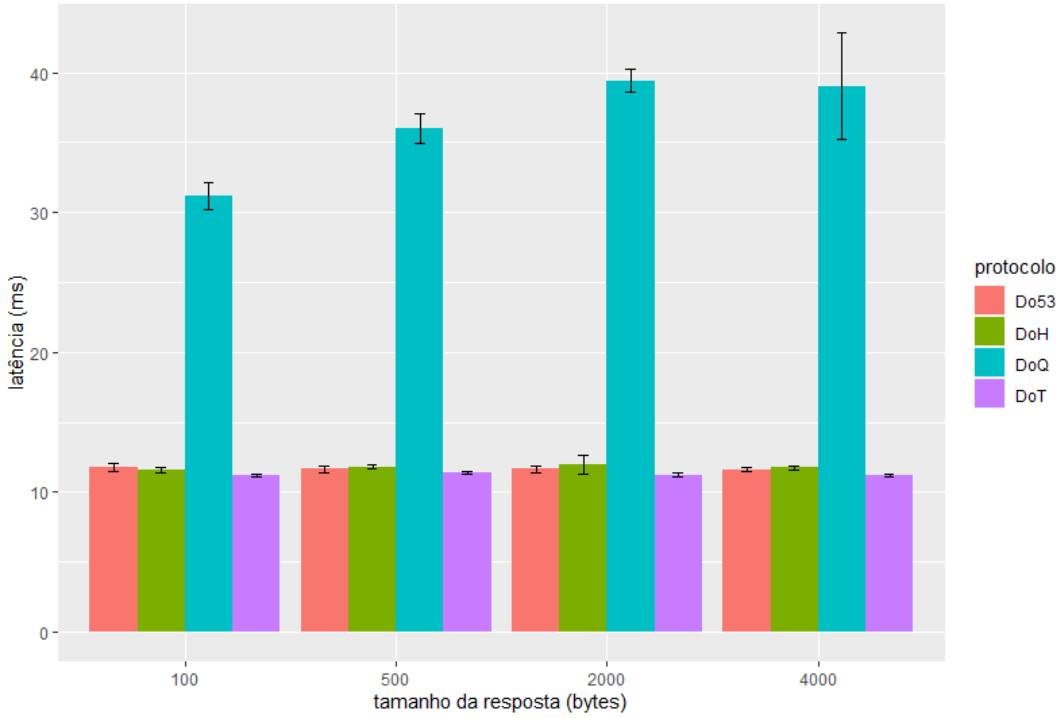

Figura 1. *Desempenho dos protocolos*

Palavras-chave: Privacidade. DNS. Protocolos de Privacidade.