Instituto de Informática (INF)
Universidade Federal do Rio Grande do Sul (UFRGS)
Porto Alegre - RS
URL: https://www.inf.ufrgs.br

Orientador: Prof. Dr. Lisandro Zambenedetti Granville
Coorientador: Dr. Eder John Scheid
Grupo de Redes de Computadores
E-mail: [granville, ejscheid]@inf.ufrgs.br

Análise e Comparação entre DNS-over-HTTPS (DoH) e DNS Clássico

1 Introdução e Motivação

O Domain Name System (DNS) é um dos principais componentes da Internet, realizando a tradução de nomes de dominio (por exemplo, *google.com*) para endereços IPs (por exemplo, `142.251.133.196`). Entretanto, esse sistema não foi criado com segurança como principal característica, resultando em diversos ataques que podem originar de servidores DNS, como flooding e spoofing [6]. Além disso, a confidencialidade das consultas DNS é afetada (e consequentemente a privacidade dos usuários também), pois toda a comunicação, por *default*, acontece utilizando texto puro [3]. Logo, atacantes e agentes não autorizados podem ter acesso a estas consultas, realizando atividades mal-intencionadas ou censurando a conexão de usuários [7].

Para resolver este problema de segurança em particular, novas soluções foram propostas, como DNS-over-TLS (DoT) [5] e DNS-over-HTTPS (DoH) [4]. Apesar destas soluções atacarem o problema de segurança, elas introduzem camadas e processos adicionais, os quais podem levar a problemas de desempenho na resolução de domínios, trocando assim desempenho por segurança [2, 1]. Portando, este trabalho visa analisar e comparar o tempo de resposta da resolução de diferentes domínios utilizando DNS clássico e DoH para quantificar tal perda de desempenho, se alguma.

2 Descrição das Atividades

Dada a introdução e motivação descrita acima, as seguintes atividades são planejadas para serem desenvolvidas durante o TG1 e TG2. É importante salientar que tais atividades podem ser alteradas durante o desenvolvimento dos trabalhos.

A1. **Estudo dos conceitos e tecnologias envolvidas**. Durante esta primeira etapa, o/a aluno(a) deverá se familiarizar com os conceitos e tópicos envolvidos no trabalho, como DNS, DoH, ataques DNS, protocolo HTTPS, e analise de dados.

A2. **Revisão bibliográfica da área.** Assim que o/a aluno(a) estiver familiarizado com os conceitos principais, ele/ela começará a etapa de investigação e análise de artigos científicos relacionados com o tema afim de mapear o estado-da-arte da área e identificar possíveis direções de pesquisa.

A3. **Definição e delimitação do escopo da solução proposta.** Esta etapa compreende a definição dos requisitos e objetivos que deverão ser atingidos pela solução, como quais domínios utilizar e quais servidores DNS. Sua delimitação deve considerar a pesquisa realizada na etapa anterior afim de propor uma solução que atendente os objetivos.

A4. **Modelagem e implementação da solução.** A solução proposta deverá ser modelada de uma maneira agnóstica a tecnologia utilizada a para a sua posterior implementação. A implementação da solução se dará como uma prova de conceito levando em conta os requisitos e objetivos listados. É crucial que a solução seja modelada com a sua posterior automatização em mente afim de realizar medições sem a intervenção de um usuário.

A5. **Coleta e Análise dos Dados.** Com a prova de conceito implementada, o/a aluno(a) irá se dedicar a coletar os dados relacionados a medições de consultas DNS e analisar os mesmos em diferentes aspectos que deverão ser discutidos com os orientadores.

A6. **Escrita do Trabalho de Conclusão.** Essa atividade é continua e deverá ser realizada ao longo de todo o trabalho conforme discussão com os orientadores. O Trabalho de Conclusão deverá apresentar de forma clara e completa o trabalho proposto e seu desenvolvimento.

As atividades deverão ser realizadas ao longo de 1 ano durante as cadeiras de Trabalho de Graduação (TG) 1 e 2. As atividades de escrita deverão ocorrer em paralelo com o desenvolvimento prático do trabalho. Sugere-se que os seguintes capítulos estejam concluídos ao final de cada uma das cadeiras:

- **TG1**: Introdução e Motivação, Referencial Teórico e Trabalhos Relacionados;
- **TG2**: Abordagem, Implementações, Avaliações e Conclusões.

Porém, tais atividades e entregas poderão ser alteradas se acordadas com os orientadores para um melhor desenvolvimento do trabalho e adequação a metas/resultados do trabalho.

3 Requisitos

- Conhecimento básico de redes de computadores;
- Conhecimento básico em Python (desejável, mas não obrigatório);
- Inglês técnico (para leitura de artigos científicos); e
- Interesse em coleta e análise de dados.

References

[1] A. Affinito, A. Botta, and G. Ventre, “Local and Public DNS Resolvers: Do You Trade Off Performance Against Security?” IFIP Networking Conference (IFIP Networking 2022), Catania, Italy, June 2022, pp. 1–9.

[2] T. Böttger, F. Cuadrado, G. Antichi, E. L. a. Fernandes, G. Tyson, I. Castro, and S. Uhlig, “An Empirical Study of the Cost of DNS-over-HTTPS,” Proceedings of the Internet Measurement Conference (IMC 2019), Amsterdam, Netherlands, October 2019, pp. 15—21.

[3] Cloudflare, Inc., “Why does DNS need additional layers of security?” 2023, https://www.cloudflare.com/learning/dns/dns-over-tls/ Acessado em 4 de Maio de 2023.

[4] P. E. Hoffman and P. McManus, “RFC 8484: DNS Queries over HTTPS (DoH),” 2018, https://www.rfc-editor.org/rfc/rfc8484.txt Acessado em 4 de Maio de 2023.

[5] Z. Hu, L. Zhu, J. Heidemann, A. Mankin, D. Wessels, and P. E. Hoffman, “RFC 7858: Specification for DNS over Transport Layer Security (TLS),” 2016, https://rfc-editor.org/rfc/rfc7858.txt Acessado em 4 de Maio de 2023.

[6] G. Schmid, “Thirty Years of DNS Insecurity: Current Issues and Perspectives,” IEEE Communications Surveys & Tutorials, Vol. 23, No. 4, pp. 2429–2459, August 2021.

[7] M. Wander, C. Boelmann, L. Schwittmann, and T. Weis, “Measurement of Globally Visible DNS Injection,” IEEE Access, pp. 526–536, May 2014.