Enhancement of DNSSec: Including Confidentiality to Name Resolution

M. T. M. Vieira, A. A. A Silva, A. E. Guelfi, M. T. de Azevedo, L. N. Marcellos, E. T. Ueda and S. T. Kofuji

***Abstract* — The Domain Name System (DNS) is one of the pillars of the Internet. Domain Name System Security Extensions (DNSSEC) is an extension that provides integrity and authentication to the service. However, despite being signed, even in DNSSEC queries are subject to unauthorized monitoring, as they are carried out using plain text, without confidentiality. The purpose of this proposal is to compare three cryptographic methods that add confidentiality to DNS queries and responses: DNSCrypt, DNS over TLS (DoT) and DNS over HTTPS (DoH). The evaluation of the results is based on the Round Trip Time of the queries and shows that despite the latency, the methods are suitable for use.**

***Index Terms* — DNS, DNSSEC, DNSCRYPT, DNS over TLS, DNS over HTTPS.**

I. Introdução

A grande razão pela qual a Internet obteve grande sucesso e tornou-se uma das mais importantes tecnologias para a comunicação, deve-se à facilidade de acesso que ela ofereceu, mesmo para aqueles com pouco conhecimento prévio sobre tecnologia. Basicamente, para acessar um *site*, basta conhecer o nome, ou endereço web, dele.

O Domain Name System (DNS) é um dos protocolos que garantiram que a Internet obtivesse o sucesso que tem hoje, já que garantiu a tradução de nomes de *sites* que as pessoas compreendam os endereços Internet Protocol [18, 19]. O DNS funciona como um serviço na Internet que faz uso de IPv4 ou IPv6 (ou ambos). Por motivo de escalabilidade, o DNS possui uma estrutura hierárquica, assim como os servidores que detém a capacidade de executar a resolução dos nomes de domínios. Uma consulta DNS de forma concisa funciona da seguinte maneira: um cliente executando uma aplicação DNS envia uma consulta DNS para algum servidor DNS com o nome a ser resolvido. Após a realização da consulta o cliente recebe como resposta o endereço IP associado aquele nome de domínio [17].

Apesar do ótimo funcionamento, um DNS possui algumas limitações fundamentais em relação à privacidade. É possível, por exemplo, que mais de um servidor armazene dados sobre um *host* ou zona. Além disso, as consultas dos nomes de domínio e as respostas transmitidas trafegam em texto aberto. Um serviço DNS também conta com algumas características que podem comprometer a segurança do serviço, como, a suscetibilidade a ataques do tipo Distributed Reflection Denial of Service (DRDoS) ou Denial of Service (DoS). Em ataques DRDoS os atacantes utilizam servidores DNS abertos de terceiros ou servidores de nome autoritativos na Internet de maneira maliciosa para o envio de consultas falsificadas para vários servidores recursivos abertos [1, 22]. Já nos ataques do tipo DoS, consultas especialmente criadas para provocar respostas grandes são direcionadas a servidores pela Internet, fato que resulta em indisponibilidade e lentidão nas vítimas [14]. Além desses, também existem os ataques de *cache poisoning* (envenenamento de *cache*) e o DNS hijacking (sequestro e redirecionamento de sessões) [10]. Claramente esses problemas estão ligados aos serviços de segurança para confidencialidade, autenticação e integridade das consultas DNS.

Para minimizar estes ataques, foi criado o DNS Security Extensions (DNSSec), que através de assinaturas digitais geradas por certificados da cadeia de servidores DNS, procura minimizar grande parte das falhas de segurança do serviço, com relação à autenticação e integridade, mas, infelizmente, não em relação à confidencialidade [3, 4].

O DNS é um componente muito importante para continuidade dos negócios para todos que utilizam a Internet. Contudo, apesar desta importância, poucos dão a devida atenção ao fato de que configurações inadequadas e falta de manutenção podem fragilizar toda a infraestrutura do serviço. Profissionais de segurança, responsáveis por proteger grandes empresas ou mesmo Internet Service Providers (ISP) muitas vezes relegam a um segundo plano, ou até mesmo ignoram, a configuração e monitoramento do serviço de DNS. Assim, o problema da falta de atualizações está sempre presente, já que, além de algumas eventuais mudanças de zona, raramente as configurações são alteradas [16].

M. T. M. Vieira, Universidade do Oeste Paulista. São Paulo, Brasil, mtuliov@gmail.com.

A. A. A. Silva, Universidade de São Paulo, São Paulo, Brasil, anderson.silva@pad.lsi.usp.br.

A. E. Guelfi, Universidade do Oeste Paulista, São Paulo, Brasil, guelfi@unoeste.br.

M. T. de Azevedo, Universidade de São Paulo, São Paulo, Brasil, marcelo.azevedo@pad.lsi.usp.br.

L. N. Marcellos, Universidade de São Paulo, São Paulo, Brasil, lincoln.marcellos@pad.lsi.usp.br.

E. T. Ueda, Instituto de Pesquisas Tecnológicas do Estado de São Paulo, São Paulo, Brasil, eduardoueda@ipt.br.

S. T. Kofuji, Universidade de São Paulo, São Paulo, Brasil, kofuji@usp.br.

O protocolo DNS foi definido em 1987 e essa longevidade explica um pouco sobre a resiliência desse serviço [18, 19]. Contudo, o fato de o DNS ser tão duradouro e os registros de domínio serem feitos para um longo prazo de validade, somado ao fato de haver poucas equipes de segurança com experiência no assunto e pouco administradores de DNS com experiência em segurança, criam um desafio único para garantir a segurança da infraestrutura desse serviço. Assim, se forem levadas em conta as ameaças internas e externas que uma organização enfrenta, a segurança DNS passa a ser um pesadelo em potencial para qualquer equipe [10].

Soma-se a estes fatos a questão da privacidade, ou seja, como o DNS trata as consultas de nomes de domínio e as respostas em texto aberto. Essas consultas podem revelar não apenas quais *sites* um indivíduo visita, mas também metadados sobre outros serviços, como os domínios de contatos de *e-mail* ou os serviços de bate-papo. Em geral, um monitoramento passivo sobre esses dados pode levantar uma quantidade enorme de informação sobre os acessos e o comportamento dos usuários. De posse dessas informações, um atacante pode utilizá-las para criação de perfis em futuros ataques [5, 10].

Diante dos problemas listados, o propósito deste artigo é implementar o DNSSec para a garantia O de confidencialidade das consultas e respostas, comparando os tempos de resposta obtidos com os tempos gerados por uma infraestrutura tradicional de DNS.

Além da motivação, das justificativas e do propósito presentes nesta seção de Introdução, este artigo está assim dividido: a seção Trabalhos Relacionados detalha pesquisas que abordam o serviço DNSSec; a seção Métodos e Materiais expõe a proposta deste artigo; a seção Experimento de Validação detalha como a validação da proposta foi conduzida; a seção Discussão dos Resultados analisa e discute os resultados obtidos; por fim a seção Conclusão traça as conclusões gerais sobre o artigo.

II. Trabalhos Relacionados

Esta seção lista trabalhos que lidam com a infraestrutura do DNSSec e são utilizados como referência para o estudo realizado neste artigo.

Os problemas de segurança decorrentes de servidores DNS que se baseiam em dados de textos abertos são tratados no artigo de [20]. Os autores propõem um cenário para implementação de um Customer Edge Switching (CES) para corrigir o problema de confidencialidade e conter varreduras e bloquear tráfego indesejado. Para contornar o problema os autores usam software DNSCrypt em conjunto com o serviço DNSSec. Os experimentos realizados comprovam que a maioria dos ataques pode ser facilmente detectada por esta contramedida, tornando recomendável a utilização de criptografia para este tipo de ambiente.

Já o trabalho [11] concentrado-se nas alterações dos padrões de consulta DNS no servidor autoritativo antes e depois das falhas de validação do DNSSec. Os autores conduzem medições controladas ativas e passivas em grande escala com sondas RIPE Atlas[1] em um servidor autorizado dedicado, para mostrar a validade desta abordagem. Os resultados demonstram que o aumento nas consultas de chave DNS (DNSKEY) é uma métrica promissora para a detecção de falhas de dados de consulta coletados passivamente. Além disso, os autores demonstram que um aumento no número de consultas é limitado mesmo para pacotes DNSSec com Time To Live (TTL) curtos. A conclusão é que valores mais curtos de TTL são benéficos na atenuação do efeito de *cache* para falhas de validação do serviço DNSSec.

Para evidenciar e tratar os problemas de segurança de DNS é proposto no trabalho de [15] a implementação de ataques comuns em um servidor DNS, com a finalidade de demonstrar que o DNSSec é uma solução eficaz para combater as falhas de segurança neste tipo de infraestrutura. A pesquisa demonstra como conter o ataque de transferência de zona por meio da geração de chaves DNSSec nos servidores de nomes, evitando que os invasores obtenham uma transferência de zona completa. O artigo também fornece um cenário detalhado de como o DNSSec pode ser usado como um mecanismo de proteção contra ataques se um invasor tentar executar o envenenamento de *cache*. Em última análise, os autores mostram que um servidor DNSSec só deve aceitar respostas autenticadas em toda a cadeia de confiança, com o descarte de respostas que vierem de entidades não autorizadas.

O trabalho de [21] utiliza a estrutura hierárquica segura do DNSSec como uma base para o estabelecimento de um serviço de Named Data Networking (NDN). O principal objetivo é atender aos interesses dos usuários por meio da nomeação de dados ao invés da localização deles na Internet. Para isso os autores criam uma Information-Centric Network (ICN) a fim de garantir a legitimidade da estrutura hierárquica de nomes e conteúdos – um problema aberto, já que não existe uma autoridade para atribuição de nomes globais na Internet (nomes, não domínios). O ponto interessante é que o trabalho serve como um validador da infraestrutura do DNSSec, já que mostra como a estrutura de hierarquia e segurança do serviço pode ser utilizada para outros fins e aplicações.

Na seção de Introdução há uma ênfase bastante grande na falta de preparação de algumas equipes que lidam com o DNS e como a falta de conhecimento pode gerar configurações inadequadas que podem se traduzir em ameaças à toda a infraestrutura de consulta do serviço DNS. O trabalho [6] vai um pouco além e mostra com alguns números muito interessantes que o problema se repete com o DNSSec. Entre os problemas listados pelos autores estão:

- Registros com erros: quase um terço dos domínios DNSSec habilitados produzem registros que não podem ser validados devido à erros;

[1] "O RIPE Atlas é uma rede global de sondas que medem ativamente a conectividade e a acessibilidade da Internet, fornecendo uma compreensão sem precedentes do estado da Internet em tempo real." - https://afrinic.net/pt/research/faq-support/what-is-ripe-atlas - acesso em 10 de outubro de 2020.

• Reutilização de chaves: em pelo menos quatro grandes provedores ocorre uma reutilização desnecessária de chaves em domínios generalizados. Nestes casos, o comprometimento de uma chave pode afetar diversos domínios. No pior caso, uma única chave é usada em cerca de 132 mil domínios;

• Política de chaves inadequada: chaves de 1024 bits, consideradas fracas em relação ao padrão de 2048 bits do NIST, são largamente utilizadas. 39% dos domínios usam chaves fracas para a assinatura de outras chaves. 70% dos domínios não trocaram as chaves no período de 21 meses;

• Validação dos registros: embora 83% dos resolvedores observados solicitem registros DNSSec durante suas consultas, apenas 12% deles realmente validam os registros.

O estudo de [6] é amplo, os autores se debruçaram sobre cerca de 150 milhões de domínios durante 21 meses. A conclusão é que a implantação de DNSSec por domínios proprietários é rara, mas está crescendo. Entretanto, há algumas práticas ruins que limitam muito a eficácia dos serviços de DNSSec. A solução recomendada pelos autores é a auditoria e a adoção de boas práticas.

As discussões levantadas nessa seção mostram como o tema DNSSec é um tema recorrente dentro da literatura científica e, de certa forma, ainda carece de pesquisas e estudos.

III. Métodos e Materiais

A proposta deste artigo envolve a implementação de um serviço DNSSec voltado para confidencialidade, autenticação e integridade. Também se pretende analisar o desempenho do serviço a partir de algumas condições e compará-lo com o desempenho de um serviço de DNS trivial. A Figura 1 mostra a arquitetura geral da proposta.

Como pode ser visto na Figura 1, a proposta contém duas operações: (1) Solicitação; e (2) Recebimento, que reúnem três componentes principais:

1. Um cliente DNS, que na operação de Solicitação recebe a consulta de uma aplicação *(browser)* e a envia ao *proxy* DNS. Este mesmo cliente DNS recebe a resposta à sua própria solicitação, ao fim da operação de Recebimento;
2. Um *proxy* DNS, que na operação de Solicitação criptografa a consulta recebida pelo cliente a envia ao servidor DNS recursivo. Da mesma forma, este mesmo *proxy* recebe a resposta criptografada do servidor recursivo e a envia ao cliente decifrada, durante a operação de Recebimento;
3. Um servidor DNS recursivo, que é encarregado de responder às solicitações do *proxy*. A estrutura é bastante simples: na operação de Solicitação o servidor DNS recebe a consulta gerada pelo cliente criptografada pelo *proxy*. Já na operação de Resposta, o servidor DNS responde à consulta criptografada.

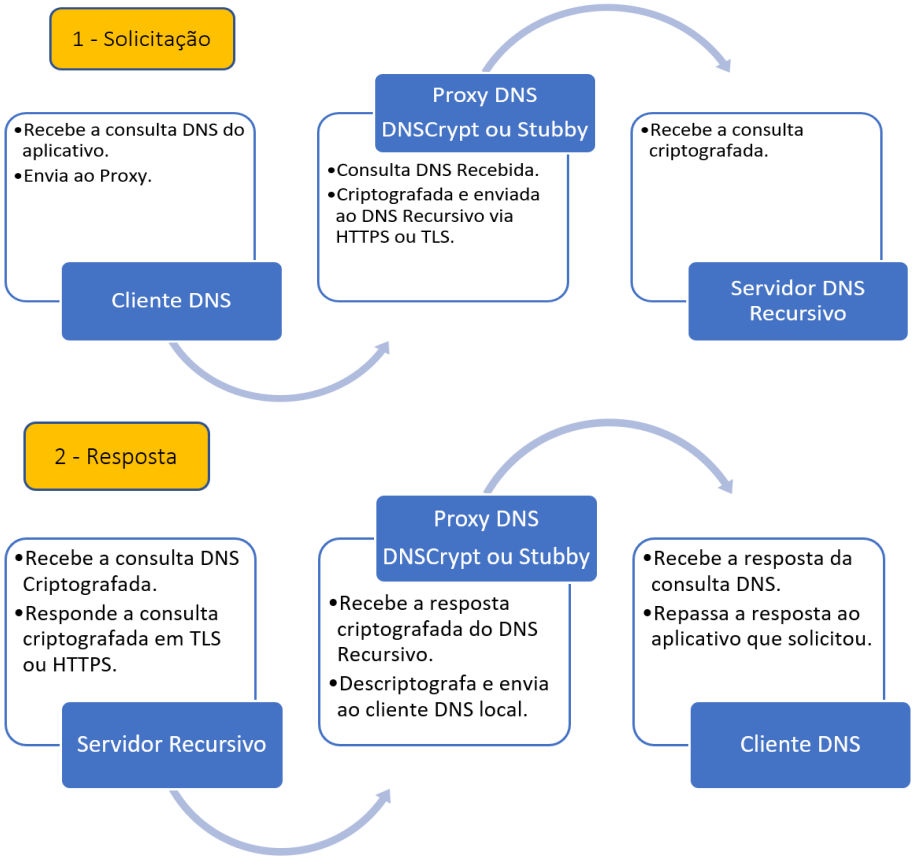

Figura 1: Arquitetura da proposta dividida nas operações de Solicitação e de Recebimento

IV. Experimento de Validação

Para validação da proposta um experimento prático de teste foi elaborado usando cenários com e sem a habilitação do serviço DNSSec. As principais especificações do experimento estão descritas na sequência.

O cliente DNS está localizado em uma rede local e está encarregado da emissão de consultas padronizadas ao servidor.

A métrica avaliada nas consultas é o Round Trip Time (RTT), que pode ser considerada uma medida de latência. A ideia é verificar se há variação da latência, comparando os resultados entre consultas a um DNS padronizado e acessos ao serviço DNSSec.

Para a criptografia o *proxy* utiliza os seguintes softwares/protocolos: DNSCrypt[2], DNS Queries over HTTPS (DoH) [10] e DNS over Transport Layer Security (DoT) [8, 9, 13].

O experimento também envolveu a medição do RTT entre estes três softwares/protocolos de criptografias. A medição do RTT tem por base os tempos de transmissão e recebimento de pacotes da rede e foi observada por meio do *sniffer* Wireshark [2]. A cada da consulta DNS criptografada foi usado o WireShark para verificar a diferença de tempo entre a consulta ao servidor recursivo do DNS selecionado e a resposta do mesmo, antes de cada consulta, foi esvaziado quaisquer registros de informações históricas do cache local, antes de iniciar as consultas para garantir que a consulta seja feita ao servidor recursivo do DNS.

O servidor DNS Recursivo é público e foi alocado na Cloudflare [7]. Para teste do DNSCrypt foi utilizado o servidor recursivo dnscript.ca-1, já que a Cloudflare não disponibiliza este software/protocolo.

A consulta padrão ao DNS é baseada no User Datagram Protocol (UDP) enquanto o DNSSec tem por base o Transmission Control Protocol (TCP) a partir do DoH e DoT, que são funcionalidades presentes na Cloudfire.

O DNSCrypt foi implementado em Windows com o software Simple DNSCrypt, que fornece uma interface gráfica para instalação e gerenciamento dos recursos e preferencias de configurações, que envolvem o método de criptografia e os servidores recursivos compatíveis com os protocolos utilizados.

Antes de cada experimento o *cache* do servidor foi esvaziado para eliminar as informações históricas dos experimentos anteriores com o comando *ipconfig /flushdns*. Os *sites* consultados, em sequência, nos experimentos são os seguintes: www.uol.com.br, d.docs.live.net, www.terra.com.br, www.unesp.br, www.usp.br, www.unoeste.br, www.abcrede.com.br.

V. Discussão dos Resultados

A execução de testes em um ambiente real, não padronizado, serve para demonstrar o desempenho objetivo dos métodos de criptografia dos serviços de DNS disponíveis, provando a viabilidade de utilização prática por parte de um usuário comum. Dessa forma, nesta seção são demonstrados e comparados os resultados obtidos com as consultas realizadas com o DNSCrypt, o DoH e o DoT.

A. Consultas com o DNSCrypt

O experimento que realiza a consulta a um servidor DNS padrão, segue um padrão básico de consultas. O cliente inicia uma sessão DNSCrypt enviando uma mensagem não criptografada. Em seguida uma consulta DNS do tipo TXT é enviada para o endereço do servidor DNS recursivo na porta DNSCrypt. A consulta inicial usa UDP, mas em caso de falha, estouro do tempo limite ou truncamento, a consulta acontece por TCP. O formato da consulta TXT para o servidor DNS padrão (sem criptografia) segue o seguinte esquema:

<nome do provedor> :: = <versão principal do protocolo>. dnscrypt-cert. <zone>.

A Figura 2 mostra o parâmetro de tempo de referência RTT de uma consulta padrão do DNS sob UDP com o DNSCrypt. Exceto por algumas anomalias, a média do RTT está registrada em cerca de 0,015ms.

Para a consulta criptografada com o DNSCrypt, o cliente envia uma consulta do tipo TXT e um nome do formulário ao servidor 2.dnscrypt-cert.example.com, como pode ser visto na Figura 3.

A zona deve ser um nome DNS válido, mas não pode ser registrada na hierarquia de DNS. Para usar um servidor DNS recursivo habilitado para DNSCrypt, um cliente deve conhecer as informações a seguir:

- O endereço IP e a porta do servidor DNS recursivo.
- O nome do provedor.
- A chave pública do provedor.

A chave pública do provedor é uma chave de longo prazo cuja única finalidade é verificar os certificados. Nunca é usada para criptografar ou verificar consultas DNS.

Como pode ser visto na Figura 4, uma resposta bem-sucedida à solicitação de certificado contém um ou mais registros, cada um contendo um certificado codificado.

As Figuras 3 e 4 mostram o processo de negociação e a troca de pacotes durante uma consulta DNS com o DNSCrypt. O cálculo e a verificação da assinatura devem incluir as extensões. Certificados criados com estas informações, sem extensões, tem 116 bytes. Com a adição do *certificado-magic, es-version e protocol-minor-version*, o registro aumenta seu tamanho para 124 bytes, como pode ser visto em destaque na Figura 4. A Figura 5 contém o RTT da consulta com o DNSCrypt.

Os destaques da Figura 5 mostram a conexão TCP estabelecida. Considerando que para cada consulta DNS usando o DNSCrypt, o processo de *three-way handshake* é realizado, nos experimentos o RTT é considerado desde o início da conexão TCP, até a resposta a solicitação da consulta DNS.

[2] O DNSCrypt é um open-source que criptografa e autêntica a comunicação entre um cliente e um servidor DNS (https://dnscrypt.info/ - acesso 17/10/2020)

No.	Time	Source	Destination	Protocol	Length	Info
1	0,000000s	192.168.0.100	1.0.0.1	DNS	74	Standard query 0x9831 A www.uol.com.br
2	0,014813s	1.0.0.1	192.168.0.100	DNS	180	Standard query response 0x9831 A www.uol.com.br CNAME dftex7xfha8fh.cloudfront.net A 54.192.57.122 A 54.1
3	7,252229s	192.168.0.100	1.0.0.1	DNS	75	Standard query 0xb571 A d.docs.live.net
4	7,266792s	1.0.0.1	192.168.0.100	DNS	173	Standard query response 0xb571 A d.docs.live.net CNAME odc-routekey-meta-geo.onedrive.akadns.net CNAME l-
5	15,101824s	192.168.0.100	1.0.0.1	DNS	76	Standard query 0x14c2 A www.terra.com.br
6	15,137518s	1.0.0.1	192.168.0.100	DNS	125	Standard query response 0x14c2 A www.terra.com.br CNAME web-portal-cdn-mia.terra.com.br A 208.84.244.116
7	23,017938s	192.168.0.100	1.0.0.1	DNS	72	Standard query 0xc9cb A www.unesp.br
8	23,032172s	1.0.0.1	192.168.0.100	DNS	107	Standard query response 0xc9cb A www.unesp.br CNAME yoda.unesp.br A 200.145.6.90
9	33,138878s	192.168.0.100	1.0.0.1	DNS	70	Standard query 0xc9ed A www.usp.br
10	33,153206s	1.0.0.1	192.168.0.100	DNS	113	Standard query response 0xc9ed A www.usp.br CNAME rubus.uspnet.usp.br A 200.144.248.41
11	55,806513s	192.168.0.100	1.0.0.1	DNS	74	Standard query 0x2393 A www.unoeste.br
12	55,821591s	1.0.0.1	192.168.0.100	DNS	111	Standard query response 0x2393 A www.unoeste.br CNAME apecnt.unoeste.br A 177.131.33.4
13	1m 20,393028s	192.168.0.100	1.0.0.1	DNS	78	Standard query 0x3858 A www.abcrede.com.br
14	1m 20,599693s	1.0.0.1	192.168.0.100	DNS	108	Standard query response 0x3858 A www.abcrede.com.br CNAME abcrede.com.br A 162.144.142.197

Figura 2: RTT Consulta DNS Padrão sob UDP com o DNSCrypt

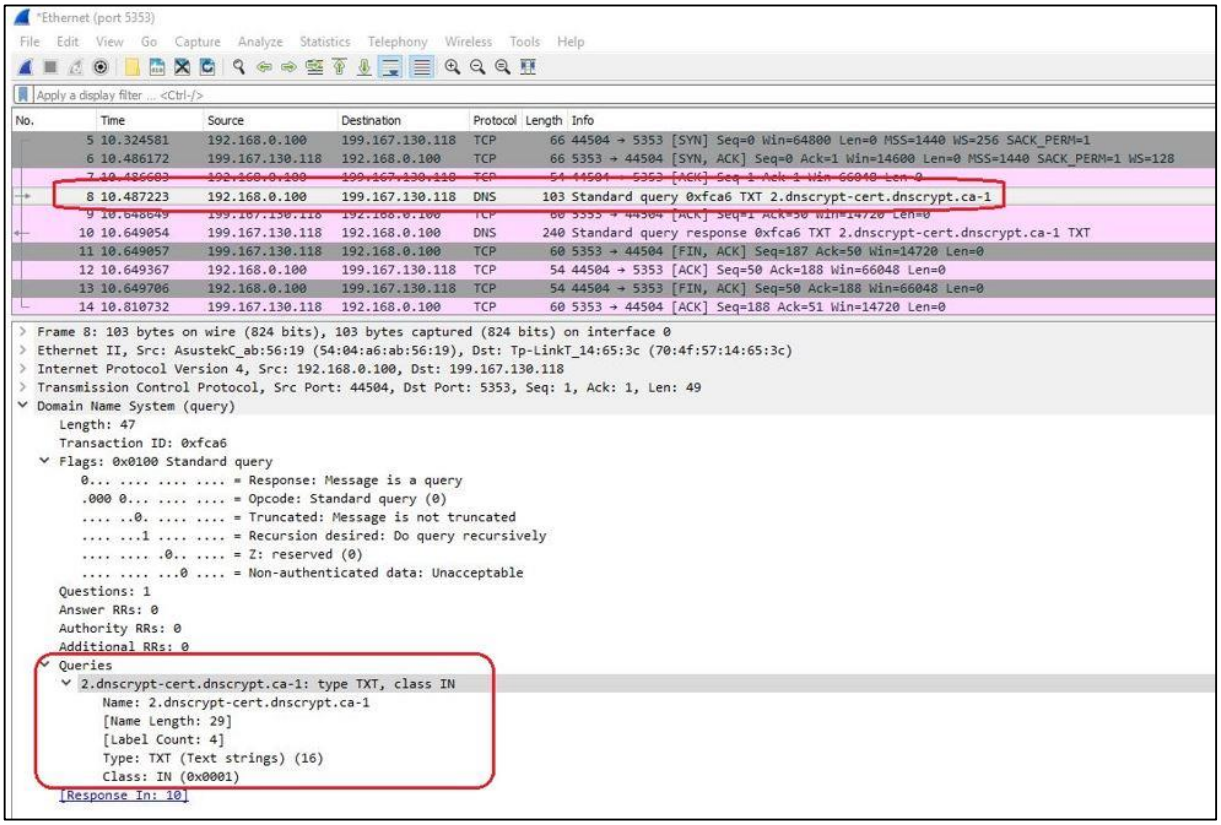

Figura 3: Solicitação da chave DNSCrypt

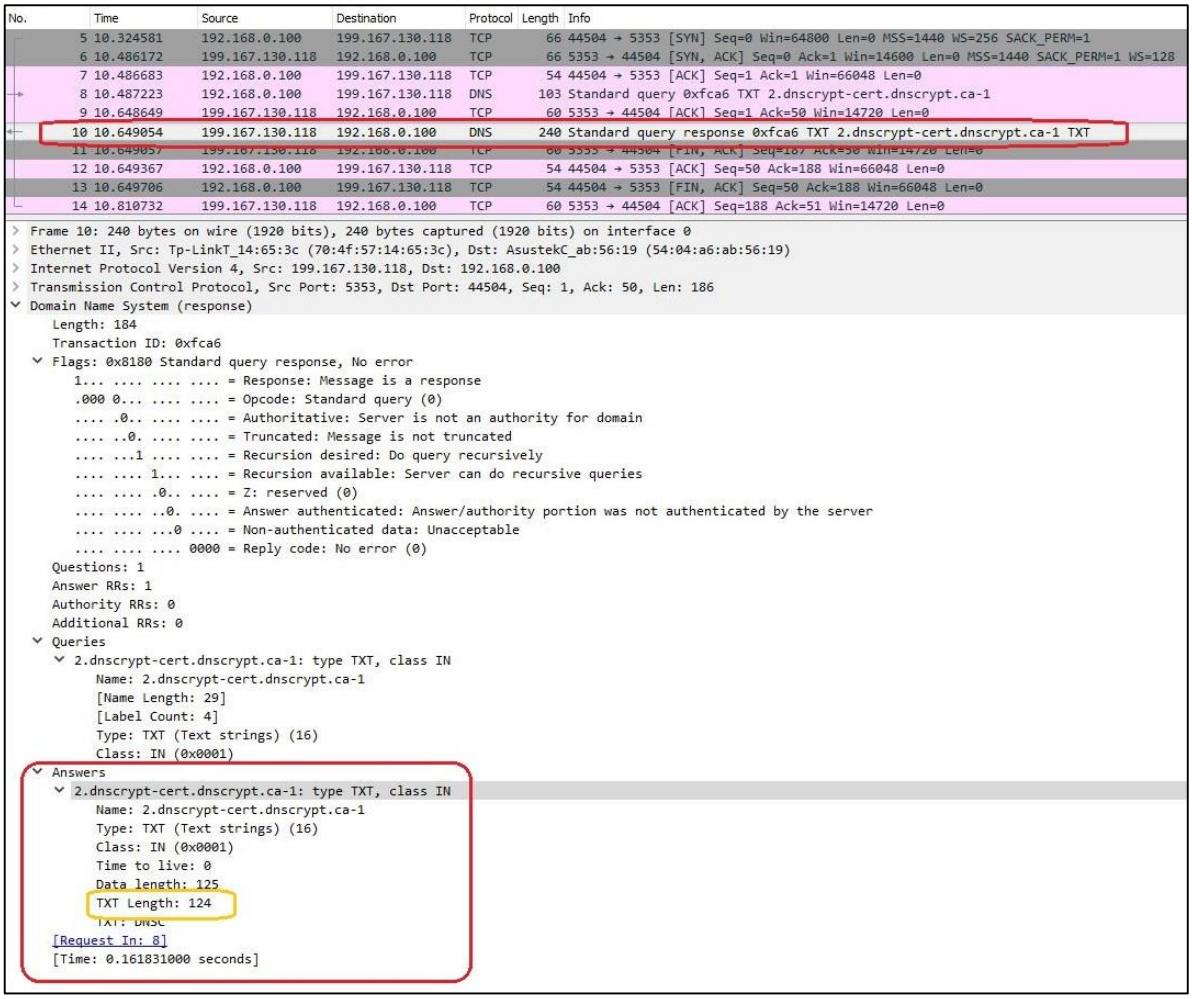

Figura 4: Resposta da solicitação da chave DNSCrypt

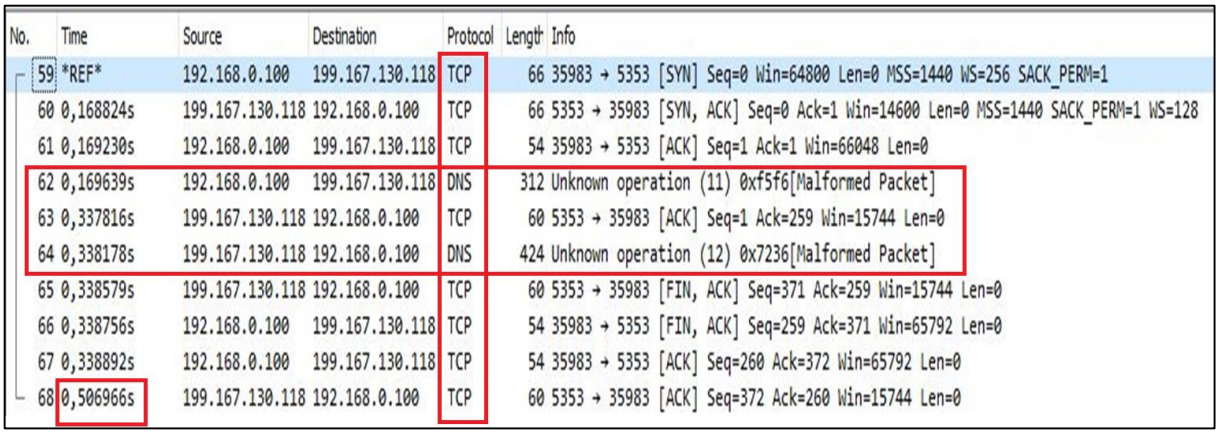

Figura 5: RTT Consulta DNS sob DNSCrypt

No destaque da Figura 5 pode-se perceber que o RTT total é de 506ms, enquanto o tempo entre a consulta e a resposta DNS, que se encontra criptografada, que é de 168ms.

A Figura 6 mostra a diferença de RTT entre a consulta DNS padrão e a consulta com o DNSCrypt.

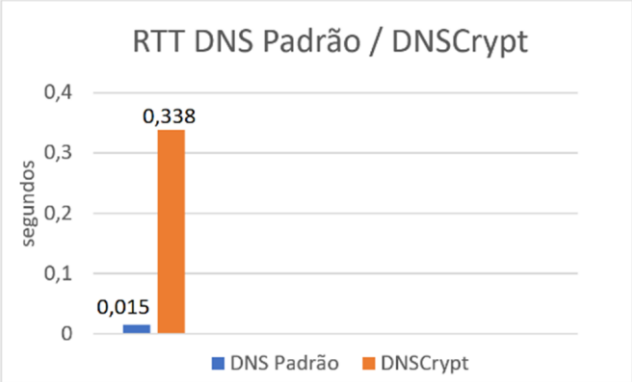

Figura 6: Tempo RTT DNS Padrão x DNSCrypt

Na Figura 6, considerando o RTT da consulta DNS padrão em comparação com a consulta DNS criptografada com o DNSCrypt, é possível observar um incremento de tempo de 323ms, ou seja, há um acréscimo de 2.253% no RTT. Alguns fatos devem ser considerados nestes números: (1) a consulta padrão do DNS é executada no servidor recursivo da Cloudflare, que é extremamente rápido por ter pontos de presença no Brasil; (2) a consulta criptografada com o DNSCrypt é realizada no servidor dnscrypt.ca-1, localizado nos Estados Unidos, California; e (3) o acréscimo do RTT causa lentidão nos acessos e consultas criptografadas. Ainda assim, é viável a utilização do DNSCrypt, dependendo claro do quão importante é para o usuário, adicionar uma camada de confidencialidade nas consultas DNS, bem como protegê-lo de ataques como DNS Spoofing e Man-in-The-Middle.

B. Consultas com o DoH

Os dados obtidos com a consulta padrão DNS usando o DoH estão exibidos na Figura 7.

Como pode ser observado na Figura 7, o tempo médio do RTT da consulta DNS padrão é de 15ms.

Para realizar o teste do RTT da consulta DNS com criptografia DoH, é utilizado o cliente DNSCrypt, que também é compatível com o padrão DoH, acessando o servidor recursivo da Cloudflare. Ou seja, o mesmo servidor utilizado na medição do RTT do DNS padrão, que disponibiliza esta modalidade de consulta DNS (DoH) de maneira pública. As medições do RTT podem ser vistas na Figura 8.

Analisando a captura da Figura 8, é possível perceber que o RTT da primeira consulta é de 62ms (pacotes 1 a 21), mas é preciso levar em consideração que nesta primeira consulta inicialmente a conexão TCP com o *three-way handshake* é realizada. Na sequência é estabelecida a conexão Transport Layer Security (TLS) e só depois disso a consulta DNS é entregue. As demais consultas, que foram feitas na mesma sequência da consulta da Figura 8 possuem um RTT bem inferior, com uma média de 15ms a 16ms. Neste caso, está estabelecido o recurso definido na RFC 8484 [12], que define que após o estabelecimento da conexão TCP/TLS, ela seja mantida aberta por um intervalo de tempo *(keep alive)*, para que as demais consultas, não sofram o impacto da latência do restabelecimento de uma nova conexão TCP/TLS.

Na Figura 9 temos a comparação dos tempos médios do RTT, tanto na consulta DNS padrão, quanto na consulta DNS usando DoH (criptografada).

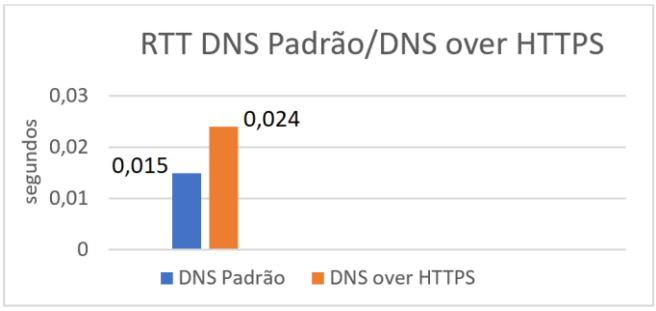

Figura 9: Tempo RTT DNS Padrão x DoH

Há na Figura 9 um incremento de 9ms no RTT médio da consulta DNS criptografada. Como neste cálculo também entra o tempo de 62ms da negociação da conexão TCP/TLS, o aumento em relação ao RTT padrão chega a 62%. Se forem consideradas as consultas após o estabelecimento da conexão, o incremento de tempo no RTT é de 1ms em média, o que é irrisório. Isso mostra que o desempenho do DNS sobre HTTPS, é diretamente proporcional à quantidade de consultas realizadas dentro de uma mesma conexão TCP/TLS. Com relação à privacidade, observa-se que todas as consultas DNS estão criptografadas com a garantia de confidencialidade.

Uma importante observação é que na Figura 7 (consulta padrão) é possível ver de forma clara os *sites* consultados, os endereços IP e as respostas do DNS. Já na Figura 8, para os mesmos *sites* essas informações não estão aparentes devido à criptografia. Não estão disponíveis dados sobre os *sites* consultados nem sobre as respostas enviadas.

Analisando os dados, fica claro que a implementação e utilização do método de consulta DoH, é viável, do ponto de vista do baixo RTT obtido.

No.	Time	Source	Destination	Protocol	Length	Info
1	0,000000s	192.168.0.100	1.0.0.1	DNS	74	Standard query 0x9831 A www.uol.com.br
2	0,014813s	1.0.0.1	192.168.0.100	DNS	180	Standard query response 0x9831 A www.uol.com.br CNAME dftex7xfha8fh.cloudfront.net A 54.192.57.122 A 54.1
3	7,252229s	192.168.0.100	1.0.0.1	DNS	75	Standard query 0xb571 A d.docs.live.net
4	7,266792s	1.0.0.1	192.168.0.100	DNS	173	Standard query response 0xb571 A d.docs.live.net CNAME odc-routekey-meta-geo.onedrive.akadns.net CNAME l-
5	15,101824s	192.168.0.100	1.0.0.1	DNS	76	Standard query 0x14c2 A www.terra.com.br
6	15,137518s	1.0.0.1	192.168.0.100	DNS	125	Standard query response 0x14c2 A www.terra.com.br CNAME web-portal-cdn-mia.terra.com.br A 208.84.244.116
7	23,017938s	192.168.0.100	1.0.0.1	DNS	72	Standard query 0xc9cb A www.unesp.br
8	23,032172s	1.0.0.1	192.168.0.100	DNS	107	Standard query response 0xc9cb A www.unesp.br CNAME yoda.unesp.br A 200.145.6.90
9	33,138878s	192.168.0.100	1.0.0.1	DNS	70	Standard query 0xc9ed A www.usp.br
10	33,153206s	1.0.0.1	192.168.0.100	DNS	113	Standard query response 0xc9ed A www.usp.br CNAME rubus.uspnet.usp.br A 200.144.248.41
11	55,806513s	192.168.0.100	1.0.0.1	DNS	74	Standard query 0x2393 A www.unoeste.br
12	55,821591s	1.0.0.1	192.168.0.100	DNS	111	Standard query response 0x2393 A www.unoeste.br CNAME apecnt.unoeste.br A 177.131.33.4
13	1m 20,393028s	192.168.0.100	1.0.0.1	DNS	78	Standard query 0x3858 A www.abcrede.com.br
14	1m 20,599693s	1.0.0.1	192.168.0.100	DNS	108	Standard query response 0x3858 A www.abcrede.com.br CNAME abcrede.com.br A 162.144.142.197
15	1m 38,950875s	192.168.0.100	1.0.0.1	DNS	75	Standard query 0xd990 A d.docs.live.net
16	1m 38,964499s	1.0.0.1	192.168.0.100	DNS	173	Standard query response 0xd990 A d.docs.live.net CNAME odc-routekey-meta-geo.onedrive.akadns.net CNAME l-
17	1m 40,211842s	192.168.0.100	1.0.0.1	DNS	93	Standard query 0x7f07 A livetileedge.dsx.mp.microsoft.com
18	1m 40,225361s	1.0.0.1	192.168.0.100	DNS	259	Standard query response 0x7f07 A livetileedge.dsx.mp.microsoft.com CNAME livetileedge.dsx.mp.microsoft.co
19	1m 56,964682s	192.168.0.100	1.0.0.1	DNS	77	Standard query 0xd705 A www.microsoft.com
20	1m 56,983678s	1.0.0.1	192.168.0.100	DNS	244	Standard query response 0xd705 A www.microsoft.com CNAME www.microsoft.com-c-3.edgekey.net CNAME www.micr

Figura 7: RTT da Consulta Padrão DNS

No.	Time	Source	Destination	Protocol	Length	Info
1	0,000000s	192.168.0.100	1.0.0.1	TCP	66	15266 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM=1
2	0,012543s	1.0.0.1	192.168.0.100	TCP	66	443 → 15266 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1 WS=1024
3	0,012768s	192.168.0.100	1.0.0.1	TCP	54	15266 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
4	0,013505s	192.168.0.100	1.0.0.1	TLSv1.2	245	Client Hello
5	0,025970s	1.0.0.1	192.168.0.100	TCP	60	443 → 15266 [ACK] Seq=1 Ack=192 Win=30720 Len=0
6	0,028160s	1.0.0.1	192.168.0.100	TLSv1.2	1494	Server Hello
7	0,028533s	1.0.0.1	192.168.0.100	TLSv1.2	1494	Certificate, Certificate Status, Server Key Exchange
8	0,028535s	1.0.0.1	192.168.0.100	TLSv1.2	60	Server Hello Done
9	0,028769s	192.168.0.100	1.0.0.1	TCP	54	15266 → 443 [ACK] Seq=192 Ack=2887 Win=66048 Len=0
10	0,033575s	192.168.0.100	1.0.0.1	TLSv1.2	139	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
11	0,046806s	1.0.0.1	192.168.0.100	TLSv1.2	97	Change Cipher Spec, Encrypted Handshake Message
12	0,046808s	1.0.0.1	192.168.0.100	TLSv1.2	115	Application Data
13	0,047008s	192.168.0.100	1.0.0.1	TCP	54	15266 → 443 [ACK] Seq=277 Ack=2991 Win=66048 Len=0
14	0,047285s	192.168.0.100	1.0.0.1	TLSv1.2	139	Application Data
15	0,047791s	192.168.0.100	1.0.0.1	TLSv1.2	261	Application Data
16	0,047873s	192.168.0.100	1.0.0.1	TLSv1.2	84	Application Data
17	0,059993s	1.0.0.1	192.168.0.100	TLSv1.2	84	Application Data
18	0,060907s	1.0.0.1	192.168.0.100	TCP	60	443 → 15266 [ACK] Seq=3021 Ack=599 Win=31744 Len=0
19	0,062501s	1.0.0.1	192.168.0.100	TLSv1.2	400	Application Data
20	0,062510s	1.0.0.1	192.168.0.100	TLSv1.2	84	Application Data
21	0,062728s	192.168.0.100	1.0.0.1	TCP	54	15266 → 443 [ACK] Seq=599 Ack=3397 Win=65536 Len=0
22	18,273427s	192.168.0.100	1.0.0.1	TLSv1.2	236	Application Data
23	18,292380s	1.0.0.1	192.168.0.100	TLSv1.2	248	Application Data
24	18,292383s	1.0.0.1	192.168.0.100	TLSv1.2	84	Application Data
25	18,292577s	192.168.0.100	1.0.0.1	TCP	54	15266 → 443 [ACK] Seq=781 Ack=3621 Win=65280 Len=0
26	29,729896s	192.168.0.100	1.0.0.1	TLSv1.2	233	Application Data
27	29,744734s	1.0.0.1	192.168.0.100	TLSv1.2	304	Application Data
28	29,744739s	1.0.0.1	192.168.0.100	TLSv1.2	84	Application Data

Figura 8: RTT Consulta DoH

C. Consultas com o DoT

O experimento com DoT, ao contrário dos experimentos com o DNSCrypt e com o DoH, usa o TCP em conjunto com o TLS ao invés do protocolo UDP. O TCP e o TLS introduzem latência ao tráfego comparado ao UDP, fato que gera um impacto negativo no desempenho do DoT. Para minimizar esta degradação no desempenho, a RFC 7858 [13] define que o cliente/Stub[3] e o servidor recursivo devem reutilizar a conexão para evitar a sobrecarga TCP/TLS que acontece em cada solicitação de DNS. Isso também é recomendado para *pipelines* com várias solicitações de DNS sequencialmente, sem que haja espera por uma resposta após cada pedido. O *Message ID*, é usado para correlacionar as solicitações com as respostas recebidas. A Figura 10 exibe o estabelecimento de uma conexão entre o cliente.

[3] Uma Remote Procedure Call (RPC) consiste na transferência do controle de parte de um processo para outra parte. Isso facilita o uso e a implementação de algumas aplicações distribuídas, eliminando a responsabilidade de servidores e clientes de lidar com sockets. Muitas RPC voltadas para a rede passam ocultas em procedimentos compostos pelo código de chamadas a rede, denominados stubs.

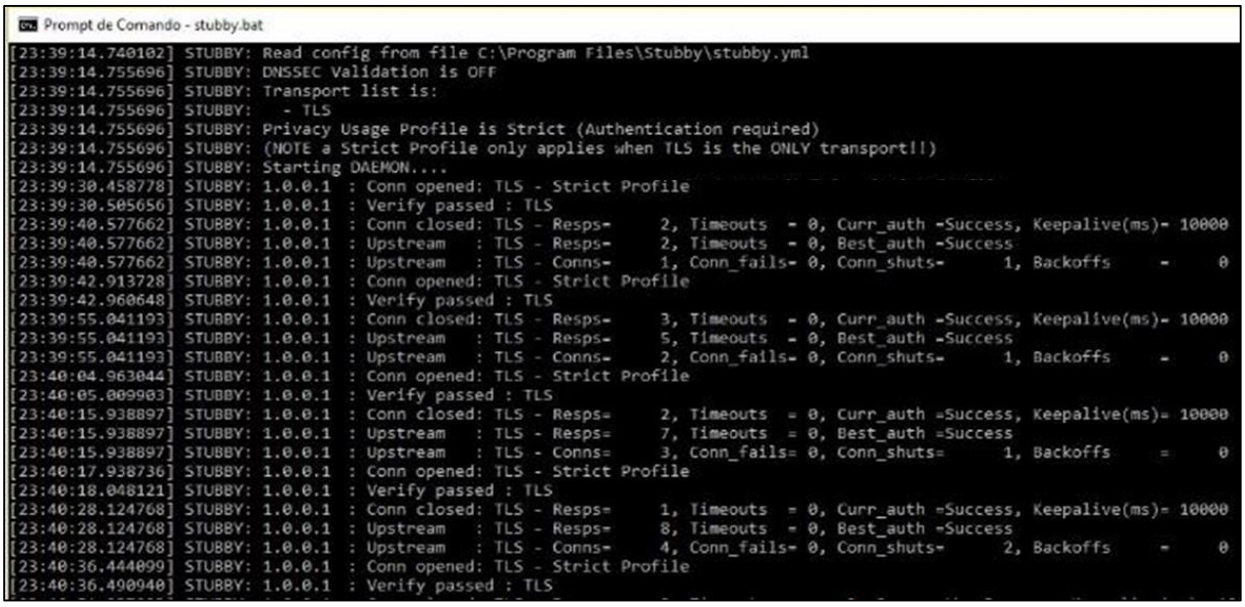

Figura 10: Estabelecimento Conexão Stubby/Recursivo

Com relação a privacidade, ao criptografar a comunicação entre o cliente/Stub e servidor recursivo, o DoT protege contra escutas nesta fase de consulta da resolução do DNS e, assim como o DoH, também protege o usuário com relação a ataques como DNS *spoofing* e *man in the middle*.

Como se pode observar na Figura 10, o software Stubby, ao estabelecer conexão com o servidor recursivo da Cloudflare define um *keepalive* em 10.000ms. Este é o intervalo de tempo que que o Stub mantém a conexão TCP/TLS aberta com o servidor recursivo para que as consultas DNS sejam feitas sem a necessidade da abertura de uma nova. Mesmo com o tempo sendo contabilizado depois da última consulta realizada, este processo diminui a latência como pode ser observado nas Figuras 11 e 12.

Na Figura 11 é observada o processo de estabelecimento da conexão (destaque 1), a consulta e resposta do DNS feita após a conexão, bem como o encerramento da conexão (destaque 2), após transcorrido o tempo estabelecido do *keepalive* de 10.000ms.

Na Figura 12, é possível observar o processo de reutilização da conexão TCP/TLS para minimizar o tempo de resposta as consultas DNS. Os destaques 1 a 4 mostram consultas e respostas DNS alternadas dentro de uma mesma conexão TCP/TLS. Também é possível observar (destaque 5) que depois de transcorridos 10.000ms, a última consulta a conexão TCP/TLS é fechada com a *flag* reset.

A Figura 13 mostra a comparação entre os tempos médios do RTT com o uso do DoT.

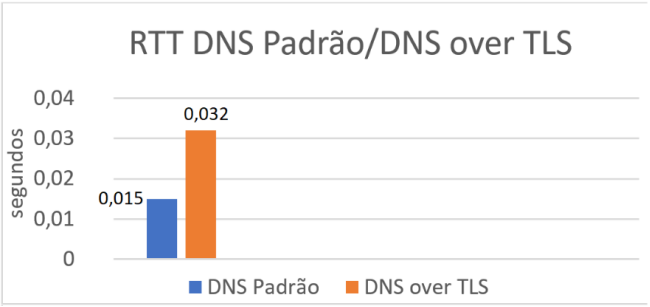

Figura 13: Tempo RTT DNS Padrão x DoT

Na Figura 13 estão tanto o RTT da consulta DNS padrão, quanto o da consulta DNS criptografada com DoT. É possível observar um acréscimo da latência de cerca de 0,017ms no RTT médio. Para o cálculo deste tempo médio, é levada em conta a negociação da conexão TCP/TLS (36ms), que representa 110% de aumento no RTT padrão. Se forem consideradas as consultas após o estabelecimento da conexão, o incremento de tempo no RTT é de 3ms em média. Tudo isso mostra que o desempenho do DoT é diretamente proporcional à quantidade de consultas feitas dentro de uma mesma conexão TCP/TLS.

De forma geral, os resultados se mostraram viáveis para uso em todos os métodos usados. O DoH conseguiu a melhor resposta de RTT (0,024s) em relação ao DoT (0,032s) e em comparação com o DNSCrypt (0,338s), que obteve a pior resposta. Com relação a privacidade, todas as consultas DNS estão criptografadas e confidenciais.

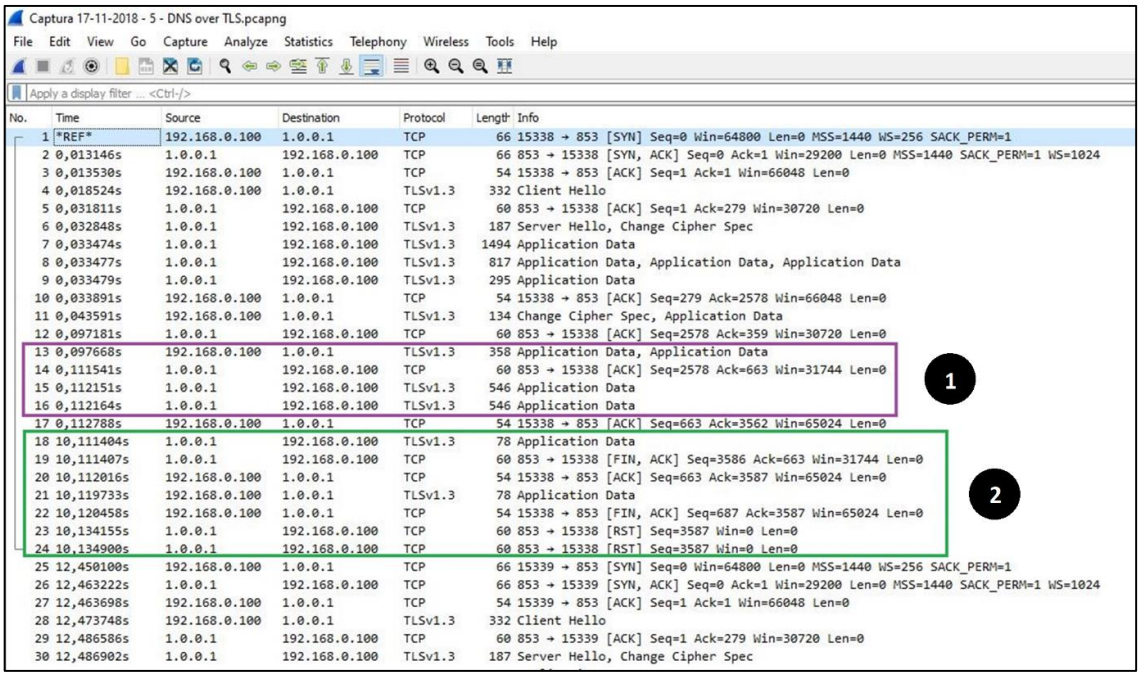

Figura 11: RTT de Uma Consulta DNS dentro em uma conexão DoT

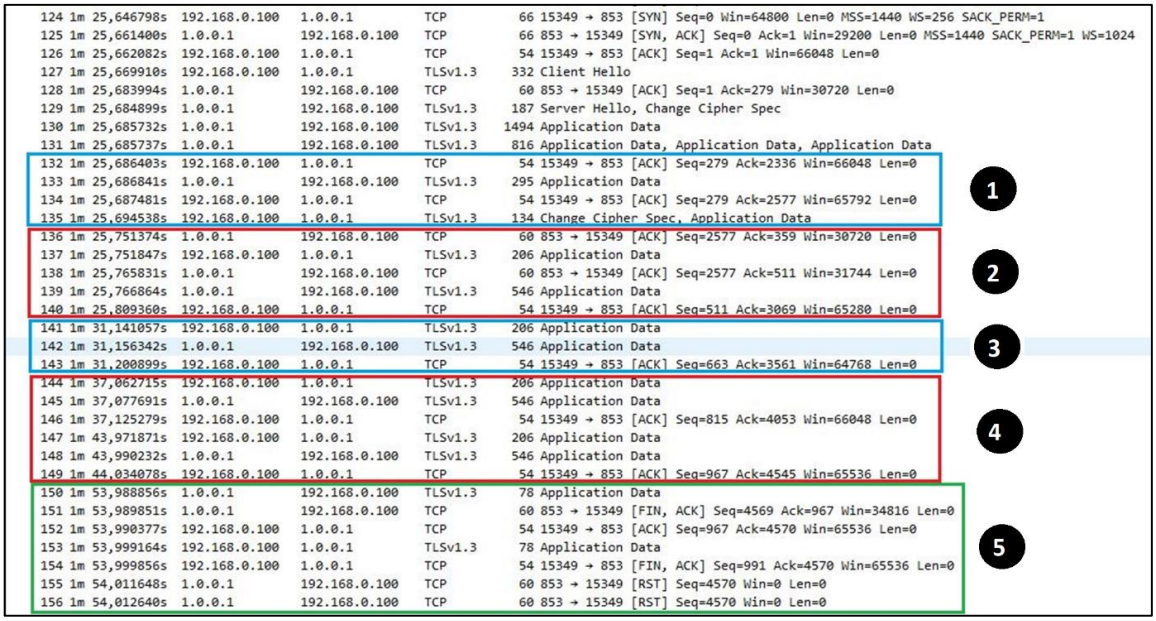

Figura 12: RTT de Várias Consultas DNS dentro da mesma conexão DoT

VI. CONCLUSÃO

Este trabalho demonstrou que o DNS pode ser uma fonte de informações valiosas para um invasor, e que, há técnicas disponíveis hoje, em desenvolvimento, que podem de maneira muito efetiva, minimizar a exposição do usuário com relação as consultas DNS. Especificamente, a proposta implementou e comparou o Round Trip Time (RTT) entre servidores DNS padronizados e criptografados (DNSSec) a partir de três métodos criptográficos: DNSCrypt, DoH e Dot. Além da autenticação e integridade, comuns em processos que envolvem o DNSSec, a avaliação tratou a confidencialidade dos dados.

Os métodos criptográficos avaliados atingem seu propósito principal de confidencialidade nas consultas DNS, porém, são suscetíveis a ataques conhecidos, inerentes aos métodos criptográficos utilizados em cada um deles. Além disso, os resultados mostraram que em detrimento à confidencialidade conseguida, a adoção dos métodos criptográficos provoca, em maior ou menor grau, algum impacto no tempo de resposta (RTT) das consultas DNS.

É importante lembrar que a proposta focou somente na primeira fase da consulta DNS, entre o cliente/stub e o servidor recursivo, ou seja, não foram contemplados neste estudo a consulta entre os servidores recursivos, os servidores autoritativos e os servidores raiz.

Também é possível constatar que os três métodos criptográficos disponíveis para implementação entre o cliente/stub e o servidor recursivo, atingiram plenamente seu objetivo, de, primariamente fornecer confidencialidade as consultas DNS entre estes dois entes do processo, e adicionalmente promoverem uma melhora significativa na proteção contra ataques conhecidos, como *Man in The Middle* e DNS *spoffing*. Uma contribuição adicional desta pesquisa é justamente ranquear o desempenho dos métodos criptográficos utilizados em relação ao RTT. O DoH teve o menor RTT médio (0,024s), seguido do DoT (0,032s) e do DNSCrypt (0,338s).

Também vale mencionar que a efetividade desta confidencialidade e proteção, passa necessariamente por uma relação de confiança entre o usuário, cliente/stub e o provedor do servidor recursivo, porque, o usuário deve confiar na assinatura pública do provedor do serviço, já que os protocolos aqui analisados não usam uma entidade certificadora para confirmação de autenticidade. Além disto, o provedor do servidor recursivo, deve ter uma política de segurança clara com relação ao não armazenamento dos *logs* das consultas DNS do servidor recursivo.

O presente trabalho abre a possibilidade de pesquisas futuras, podendo os trabalhos futuros abordarem novos ataques, que não contemplados no presente estudo, contra o DNSSEC. Comparação de medidas de contenção e mitigação de ataques de negação se serviços é um campo que pode ser explorado, além de estudos de outras implementações de DNSSEC na proteção da resolução de nomes.

REFERÊNCIAS

[1] ALIEYAN, K.; KADHUM, M .M.; ANBAR, M.; REHMAN, S. U.; ALAJMI, N. K. A. An overview of DDoS attacks based on DNS, International Conference on Information and Communication Technology Convergence (ICTC), 2016, pp. 276-280, doi: 10.1109/ICTC.2016.7763485.

[2] ANALYZER, Wireshark Network Protocol. Disponível em < http://www. wireshark. org>. Acesso em 10 de outubro de 2020.

[3] ARENDS, R.; AUSTEIN, R.; LARSON, M.; MASSEY, D.; ROSE, S. Resource Records for the DNS Security Extensions, RFC 4034, 2005.

[4] ARENDS, R.; AUSTEIN, R.; LARSON, M.; MASSEY, D.; ROSE, S. Protocol Modifications for the DNS Security Extensions, RFC 4035, 2005.

[5] BORTZMEYER, S. DNS Privacy Considerations, RFC 7626, 2015.

[6] CHUNG, Taejoong et al. A longitudinal, end-to-end view of the DNSSec ecosystem. In: 26th USENIX Security Symposium (USENIX Security 17). 2017. p. 1307-1322.

[7] CLOUDFLARE. Plataforma global de nuvem. Disponível em <htttp://www. cloudflare.com>. Acesso em 10 de outubro de 2020.

[8] DICKINSON, J.; DICKINSON, S.; BELLIS, R.; MANKIN, A.; WESSELS, D. DNS Transport over TCP - Implementation Requirements, RFC 7766, 2016.

[9] DICKINSON, S.; GILLMOR, D.; REDDY, T. Usage Profiles for DNS over TLS and DNS over DTLS, RFC 8310, 2018, 27 pp. Dispnível em https://datatracker.ietf.org/doc/html/rfc8310. Acesso em 17 de outubro de 2020.

[10] FARRELL, S.; TSCHOFEING, H. Pervasive Monitoring Is an Attack, RFC 7258, 2014.

[11] FUKUDA, K., YONEYA, Y., MITAMURA, T. Towards detecting DNSSEC validation failure with passive measurements, IEEE/IFIP Network Operations and Management Symposium, 2020, pp. 1-6, doi: 10.1109/NOMS47738.2020.9110466.

[12] HOFFMAN, P.; MACMANUS, P. DNS Queries over HTTPS (DoH), RFC 8484, 2018, 21 pp. Disponível em https://www.rfc-editor.org/rfc/rfc8484.txt. Acesso em 17 de outubro de 2020.

[13] HU, Z. et al. Specification for DNS over Transport Layer Security (TLS), RFC 7858, 2016, 18 pp. Dispnível em https://datatracker.ietf.org/doc/html/rfc7858. Acesso em 17 de outubro de 2020.

[14] JINGNA, L. An analysis on DoS attack and defense technology, 7th International Conference on Computer Science & Education (ICCSE), 2012, pp. 1102-1105, doi: 10.1109/ICCSE.2012.6295258.

[15] KHAN, I.; FARRELLY, W.; CURRAN, K. A Demonstration of Practical DNS Attacks and their Mitigation Using DNSSec. International Journal of Wireless Networks and Broadband Technologies (IJWNBT), 2020, 9(1), 56-78.

[16] LISKA, A.; STOWE, G. Segurança de DNS: Defendendo o Sistema de Nomes de Domínio, 1a Ed. São Paulo: Novatec, 2016. 298.

[17] LYNN, M. S. A Unique, Authoritative Root for the DNS. The Internet Protocol Journal, v. 4, n. 3, 2001. Disponível em: <https://www.icann.org/resources/pages/unique-authoritative-root-2012-02-25-en>. Acesso em 17 de outubro de 2020.

[18] MOCKAPETRIS, P. Domain Names – Concepts and Facilities, RFC 1034, 1987.

[19] MOCKAPETRIS, P. Domain Names – Implementation and Specification, RFC 1035, 1987.

[20] NOWACZEWSKI, S.; MAZURCZYK, W. Securing Future Internet and 5G using Customer Edge Switching using DNSCrypt and DNSSec. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 2020, 11(3), 87-106.

[21] TEHRANI, P. F.; OSTERWEIL, E.; SCHILLER, J. H.; SCHMIDT, T. C.; WÄHLISCH, M. The Missing Piece. Proceedings Of The 6Th Acm Conference On Information-Centric Networking, [S.L.], 24 set. 2019. ACM. http://dx.doi.org/10.1145/3357150.3357401.

[22] YU, S., Distributed denial of service attack and defense, Springer, 2014, New York, N.Y., doi: 10.1007/978-1-4614-9491-1.

Marco Túlio Manso Vieira é especialista em Segurança da Informação (2018) e Tecnólogo em Redes de Computadores (2015), ambos pela Universidade do Oeste Paulista (UNOESTE/SP). Atualmente é consultor de Infraestrutura e Segurança da Informação, atuando em empresas de diversos segmentos de negócio e porte.

Anderson Aparecido Alves da Silva recebeu o título de Doutor em Engenharia da Computação pela Universidade de São Paulo (USP) em 2016, Mestre em Engenharia da Computação pelo Instituto de Pesquisas Tecnológicas do Estado de São Paulo (IPT) em 2010, Especialista em Administração de Empresas - Análise de Sistemas pela Fundação Escola de Comércio Álvares Penteado (FECAP) em 1993, e Graduado em Processamento de Dados pelo Centro Universitário FIEO (UNIFIEO) em 1991. Trabalhou como gerente de TI por 23 anos. Atualmente desenvolve projeto de pós-doutorado em segurança de aprendizado de máquina na Universidade de São Paulo (USP) e é professor em instituições paulistas (IPT, UNIP, SENAC).

Adilson Eduardo Guelfi é Doutor em Engenharia Elétrica pela Universidade de São Paulo - USP (2002), Mestre em Engenharia Elétrica pela Universidade Federal de Santa Catarina - UFSC (1998), Especialista em Gestão de Negócios e Projetos pela Faculdade FIA de Administração e Negócios - FIA (2009), e Bacharel em Engenharia Elétrica pela Escola de Engenharia de Lins – FPTE (1996). Adilson atuou como gerente técnico do LSI-TECH e atualmente ocupa o cargo de Pró-Reitor de Pesquisa e Pós-Graduação da Universidade do Oeste Paulista - UNOESTE/SP.

Marcelo Teixeira de Azevedo possui doutorado e mestrado em Engenharia Elétrica pela Escola Politécnica da Universidade de São Paulo (EP-USP), em 2017 e 2010, respectivamente. Também possui MBA em Gestão de Pessoas e Liderança pela Faculdade Jardins – FAJAR (2017) e Graduação em Ciência da Computação pela Universidade Santa Cecília – UNISANTA (1999). Atualmente é docente na Faculdade de Santa Bárbara d'Oeste, no curso de Engenharia de Controle e Automação. Seus interesses de pesquisa incluem Internet das Coisas, Indústria 4.0, Redes de Comunicação e Cibersegurança.

Lincoln Nogueira Marcellos possui doutorado em Ciências Sociais pela Pontifícia Universidade Católica de São Paulo – PUC/SP (2012), mestrado em Administração pela Universidade Municipal de São Caetano do Sul – USCS (2006), especialização em Planejamento, Implementação e Gestão da Educação a Distância pela Universidade Federal Fluminense – UFF (2019), graduações em Administração de Empresas e em Ciências Econômicas pelo Centro Universitário Santo André – CUFSA, em 2005 e 2004, respectivamente, e graduação em Direito pela Faculdade de Direito de São Bernardo do Campo – FDSBC, em 2002. Atualmente é pós-doutorando junto ao PAD/LSI - Universidade de São Paulo (USP.)

Eduardo Takeo Ueda é Doutor em Engenharia Elétrica pela Escola Politécnica da Universidade de São Paulo – EP/USP (2012), Mestre em Ciência da Computação pelo Instituto de Matemática e Estatística da Universidade de São Paulo – IME/USP (2007), Especialista em Informática em Saúde pela Escola Paulista de Medicina da Universidade Federal de São Paulo – EPM/UNIFESP (2014), Graduado em Engenharia de Computação pela Universidade Virtual do Estado de São Paulo – UNIVESP (2019), e Graduado em Matemática pela Universidade Estadual Paulista – UNESP (2000) . Atualmente é Professor no Centro Universitário Senac de São Paulo (SENAC), e Professor/Orientador do Programa de Mestrado Profissional em Computação Aplicada no Instituto de Pesquisas Tecnológicas do Estado de São Paulo (IPT). Suas linhas de pesquisa são Criptografia e Segurança da Informação, com interesse principalmente nos seguintes temas: Algoritmos e Protocolos Criptográficos, Modelos de Autenticação e Autorização, e Técnicas de Inteligência Artificial em Cibersegurança.

Sergio Takeo Kofuji é Doutor e Mestre em Engenharia Elétrica pela Escola Politécnica da Universidade de São Paulo – EP/USP, em 1995 e 1988, respectivamente, e Bacharel em Física pelo Instituto de Física da Universidade de São Paulo – IF/USP (1981). Atualmente é Professor Doutor da Escola Politécnica da Universidade de São Paulo. Também é Pesquisador Associado do InovaUSP e Coordenador do Grupo de Pesquisa do CNPq "Computação Pervasiva e de Alto Desempenho". Atua principalmente nos seguintes temas: Computação Pervasiva, Redes de Sensores Sem Fio, Grades Computacionais de Armazenamento (DataGrids, GridServices), Processamento Paralelo, Processadores (SMT, CMP, PIM), Simuladores de Processadores (Programação no Cell), Arquitetura Reconfigurável, Sistemas Ciber-Físicos e Embarcados, Imageamento IR, UWB e ondas milimétricas, Computação Móvel e Sem Fio, e Redes de Alta Velocidade.