Advantages of DNS-over-HTTPS over DNS

Hrushak Serhii[1]

Pavlenko Cynthia[2]

[1]National Aviation University, 56 Zodchykh street,
Kiev UA-03162, Ukraine, sg.grusha@ukr.net

[2]National Aviation University, 56 Zodchykh street,
Kiev UA-03162, Ukraine, neesmu13@gmail.com

Abstract. *Today information security concerns stand as the main topic in many computer-related fields. This work describes new standardized protocol: DNS-over-HTTPS. Encryption of DNS queries, pros and cons of new protocol, should we prefer DNS-over-HTTPS or just use old DNS? Let us try to figure it out.*

Keywords: *network; transmission of data; encryption of data; security; DNS; DNS-over-HTTPS.*

I. Introduction and Problem statement

Domain Name System (DNS) – simple query-response protocol. Its main purpose is to name computers, services and other resources that connected to the Internet or private networks [1]. It translates human-readable domain names to corresponding IP addresses and so locates computer services with the underlying network protocols.

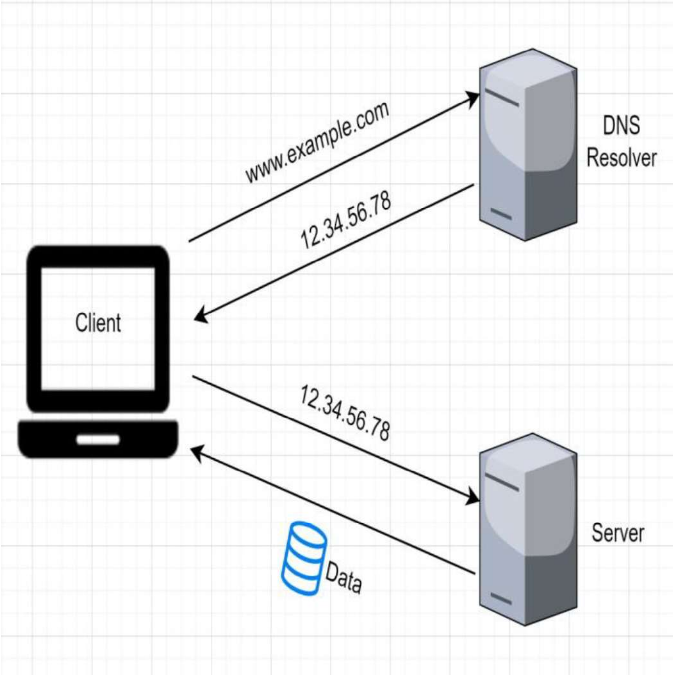

Figure. 1. Domain name resolving via DNS protocol

Nowadays, flow of data between computers constantly increases. As a result, needs in secured data transmission channels between them also increase. Theft of sensitive and private information can be disastrous for any private person or company. They may not even know that they use DNS every day, which does not determine the proper protection when transferring queries over Internet.

This work will tell about DNS-over-HTTPS protocol and its advantages over classical DNS.

II. Problem solution and Results

DNS-over-HTTPS – is a protocol for performing remote domain name resolving via the HTTPS protocol [1]. Main goal of protocol is to increase user privacy and security by preventing eavesdropping and manipulation of DNS data by man-in-the-middle attacks (MITM). MITM attack is active eavesdropping, in which attacker creates independent connections between client and remote service, in that way relaying messages between them to make them believe that they are talking directly to each other over a private connection [2]. Such interconnection layer (man-in-the-middle) can read and change any data that goes through.

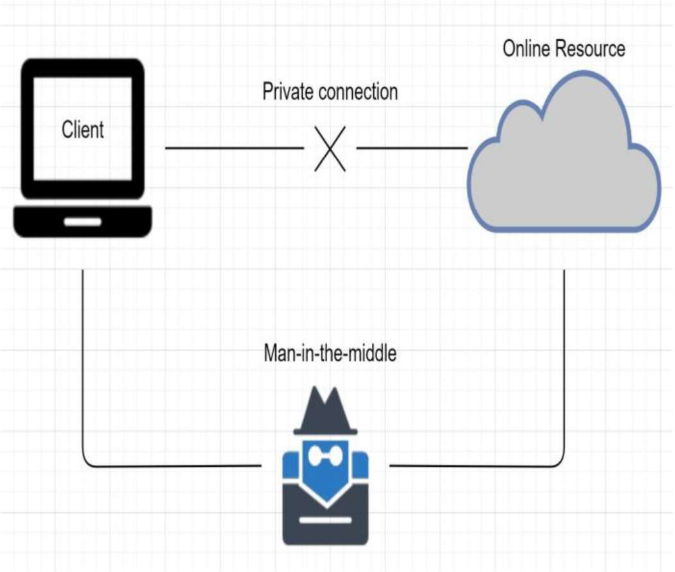

Figure. 2. Basic concept of man-in-the-middle attack

DNS-over-HTTPS requests/responses are handled over standard SSL port – 443. Protocol allows using two methods of HTTP requests: GET and POST. When using POST method original DNS query must be placed in body section of the message. Content-Type request header field must indicate the media type of the message. Protocol defines a new Content-Type request header for this – *application/dns-message*. Queries exchange between client and DNS-over-HTTPS server can be cached accordingly to HTTP and/or DNS basic cache rules.

Encryption of DNS-over-HTPS queries are done “on-fly” right before transmitting data between endpoints. Basic concept behind this procedure is beforehand established SSL connection between client and DNS-over-HTTPS server. SSL connection begins at handshake, which goals are to satisfy that client talks to the right server and vise-versa; agree on using encryption algorithm they will use to exchange data; agree on necessary keys for chosen algorithm [3]. After establishing SSL connection, client encrypts data before transmitting it to the server and vice-versa.

Let us review some pros and cons of DNS-over-HTTPS protocol. Pros are: makes MITM attacks useless; obfuscated data can't be sniffed by third-parties; all data flow is done using traditional SSL 443 port, so DNS queries can't be distinguished from traditional HTTPS queries; DNS traffic is centralized on a few DNS-over-HTTPS servers that may lead to improved load time performance. Cons are: makes traditional DNS-filtering practically useless; is not widespread today, so it lacks support [4]; decreases overall Internet cyber-security, because it makes harder to monitor suspicious activity [5].

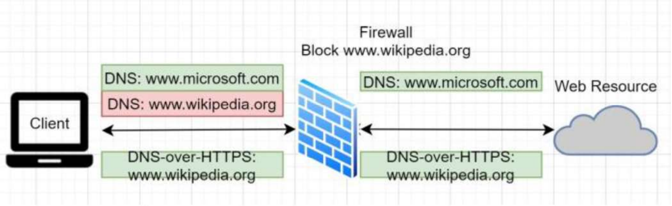

Figure 3. Firewall DNS-filtering outflank

III. Conclusions

DNS-over-HTTPS protocol closes Internet web-browsing security gaps by introducing encryption between DNS-clients and DNS-resolvers. Protocol intends transmitting queries over common HTTPS protocol and works with its standard rules.

As any new technology or protocol, DNS-over-HTTPS traditionally solves some problems and brings new ones. But one can be said for sure: it can become a new de-facto standard for DNS-resolving in the near future.

References

[1] Adam Roach, Benjamin Schwartz, RFC 8484 - DNS Queries over HTTPS (DoH), 2018, p. 21.

[2] Richard Chirgwin, IETF protects privacy and helps net neutrality with DNS over HTTPS, 2017.

[3] A. Freier, RFC 6101 - The Secure Sockets Layer (SSL) Protocol Version 3.0, 2011, p. 67.

[4] Lawrence Abrams, Google Unveils DNS-over-HTTPS (DoH) Plan, Mozilla's Faces Criticism, 2019.

[5] Zack Whittaker, Internet group brands Mozilla 'internet villain' for supporting DNS privacy feature, 2019.