IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 10, October 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910015 |

QUIC - Improving the Transport and Security of the Domain Name System

Purvansh Jain[1], Dr. Manjunath C R[2], Vishwajeet Sharma[3], Ritwika Dhal[4]

UG Students, Dept. of CSE, JAIN (Deemed-to-be-University), Bengaluru, Karnataka, India[1,3,4]

Associate Professor, Dept. of CSE, JAIN (Deemed-to-be-University), Bengaluru, Karnataka, India[2]

ABSTRACT*:* In the cutting edge world, individuals are progressively sending information over the network in the real world, which means tremendous benefit. Anything involves the transfer through the network of sensitive details such as passport information and credit card data, in the form of online shopping, paying the penalty, and booking a ticket in the film. The heart of the internet is known as the Domain Name System (DNS).Today, it is one of the foundational elements of the internet. DNS is one of the key components in the internet which acts as a starting point and informs you of the relevant IP addresses associated with domain names in day-to-day communication. The usage of DNS is not only for translating names and addresses and vice-versa but also for various security service improvements. Hence, protecting and securing the Domain Name System is one of the key interests in the arena of Cyber Security. The security of the transmission of the data relies upon the chance of the further presentation of PC advances in human existence. The paper presents an analysis and application of various protocols for improving the security and transport of the DNS System making the secure deployment and configuration procedures for the system that will be used in production. A new experimental transport protocol QUIC is developed, the system should not offer a client to wait for a longer time to get its response, also not degrading the security. Balance between the security and performance has to be achieved. The increasing level of applications and devices should require a well-defined application that generates a balance

KEYWORDS*:* Domain Name System; Transport Layer Security; Quick UDP Internet Connections; DNS Over TLS; DNS over HTTPS; Transmission Control and User Datagram Protocol; Domain Name Systems Security Extensions; DNS Over QUIC; Transaction Signature; Application Layer Protocol Negotiation

I. INTRODUCTION

People are transmitting data more and more across the network in the real world, which means tremendous benefit. Anything involves the transfer through the network of sensitive details such as passport information and credit card data, in the form of online shopping, paying the penalty, and booking a ticket in the film [1]. The safety of this knowledge depends on the likelihood that computing devices may further be introduced in human life. Data networks now use many protocols to ensure secure communication transmission, but in all cases, they cannot provide full security [2].One of the basic building blocks of Internet Protocol (IP) communications is the Domain Name System (DNS). DNS focuses on the improved usability of the IP Communications System. One of the very generic uses of the system is to enable users to use user-friendly domain names, instead of complex numbers. In order to participate in the IP communication, numeric addresses are preferred. Hence, DNS here plays a key role in enabling the user to use a friendly name and the Domain Name System helps in mapping it to numeric addresses.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910015 |

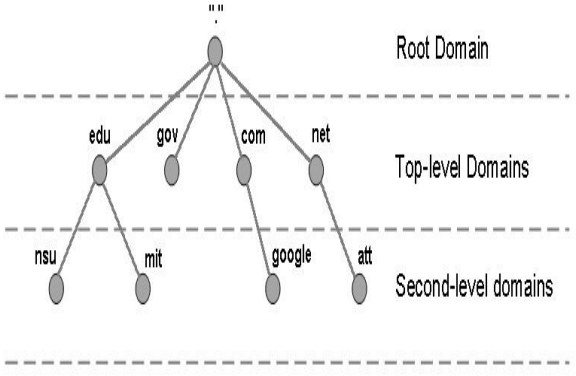

FIG-1 – DNS HIERARCHY

The system also helps the administrators to map names and numbers with ease. By handling the activity to the DNS. Using the DNS fig-1, we would be able to map 192.0.1.8 today and later change it to 192.0.1.9 without affecting any end users. The system solves by enabling them to do a DNS lookup, thus further enabling them to communicate. The IP Addresses can be changed as needed whenever and wherever possible. Being a Network Service, DNS has evolved from a simple lookup utility that serves name and IP Addresses, to a very complex supporting data, multimedia, voice and even security applications. The DNS is extremely scalable for such uses and applications.

Hence there exist a lot of loopholes in the system which paves a way for attackers to make changes, thereby posing a threat to confidentiality, integrity and availability of the service.If the DNS server is not set properly, the DNS problems exist. A vital role is played by DNS and name servers in internet communication overall. DNS is in widespread usage on different platforms, across multiple operating systems, with varied software applications, various operators, and a wide range of technical expertise. For security, the system must be made immune to hostile threats andattacks. Security problems will be overcome by using a well-planned secure deployment strategy.

TLS - TRANSPORT LAYER SECURITY

The Transport Layer Security (TLS) protocol secures the Internet by providing cryptographic services. This data transmission is done by setting up a simple TCP connection over an encrypted channel. When the client trusts the web server, the server will be verified using the digital certificate, thus proving the validity of the web server.

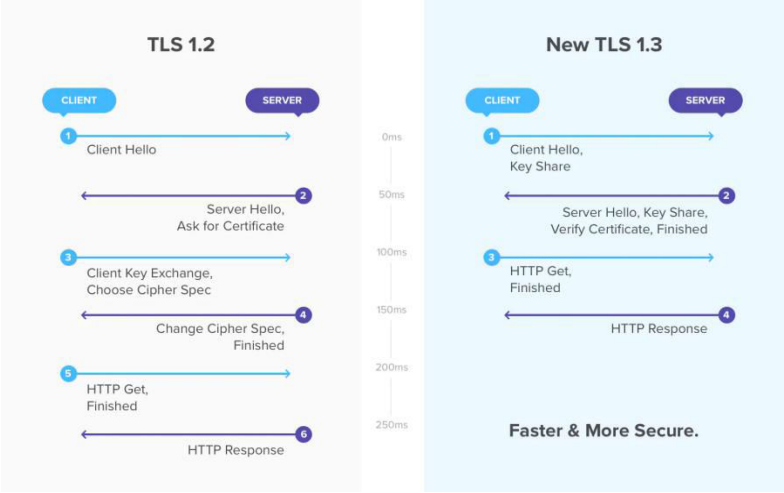

FIG-2 TRANSPORT LAYER SECURITY

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910015 |

In fig-2, the handshake protocol, the trust is built via a secret key established by negotiating a handshake between a web client and web server. It allows users to maintain control of their personal data and to help guarantee a secure transaction.

Before the TLS protocol all transactions were using the SSL protocol and due to too many security flaws they introduced TLS protocol with existing features as well as SSL 3.0 features. TLS relies on key exchange mechanisms to establish secure sessions. TLS just sits on top and secures the handshake process. TLS v1.3 is way faster and the handshake is also simpler and faster than its predecessors.

II. PROBLEM DEFINITION

The current transactions of the Domain Name System happen largely over UDP. The generic transaction mechanism which it has is totally "un-encrypted"! Any malicious actor can tamper with the data and apply and reply accordingly. This creates very big and strong loopholes in the form of various server-side attacks, transit-level attacks & client-side attack in the system causing the issues in Confidentiality, Integrity and Availability of the system.These issues have been addressed by employing DNS security extensions such as DNS over HTTPS (DoH), DNS over TLS (DoT), and several other security enhancements to the system. A lot of security mechanisms including the encryption system which is used in the transport may cause overheads. The overhead elimination has to be carried at the other level than the client level.

The proposed work in paper aims to deliver a guide that mainly focuses on the secure deployment and improved transport protocol for the safe and low-latency transactions on the Domain Name System. The works provides an idea of the implementation strategy of the newer protocols at the both server side and client side, thus making the system more fast and secure, and also delivers the configuration and delivery of knowledge of various protocols and applications which are industry-standard, which aim at safe and best practices.

III. QUIC - THE FUTURISTIC PROTOCOL

Unlike TCP, which has a high latency, QUIC (Quick UDP Internet Connection) is an upgrade which is designed to lower latency.A UDP-based protocol very similar to TCP, TLS, and HTTP/2 is being implemented as QUIC. TCP uses 3-step handshake protocol and if you combine it with TLS it increases the number fig-3. QUIC uses UDP as its basis, optimized for HTTP/2 semantics and TLSv1.3 by default.

The new transport is based on UDP, and therefore it has equal flow control, in the same manner as HTTP/2, and also comparable security, comparable to TLS and Record layer encryption.When it comes to reliability, features like efficiency,congestion semantics and advanced handling of network congestion are quite comparable to TCP.

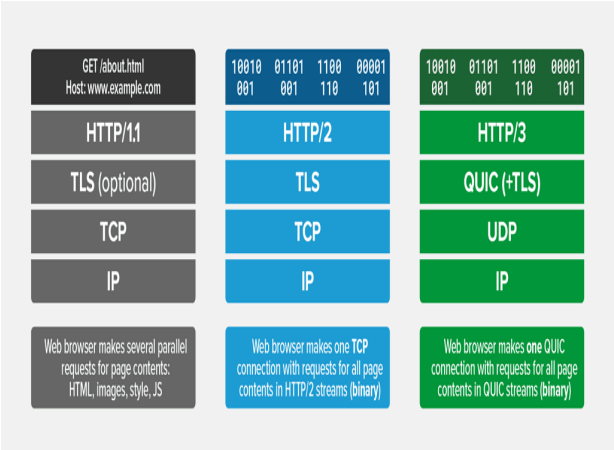

FIG-3 Comparision between HTTP/1.1, HTTP/2, HTTP/3

QUIC for DoH and a new DoQ:

i. TLS + TCP + Streams = Functionality.
ii. TLS version 1.3 used to establish and encrypt all packets (Include ACKs) and session keys.
iii. The DoH can make use of HTTP/3 for very efficient data transfer over others.
iv. The DoQ can make use of QUIC - Streams for very efficient data transfer over others.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910015 |

v. RTT connection establishment ratio is 0% when we compare with the TLS.

IV. IMPLEMENTATION

The Hardware setup: Virtual Machines have their specifications 2.3 GHz, 1 GiB RAM, 8 GiB of storage. The Operating System installed is a Linux-based distribution, Ubuntu 20.04 LTS. Network bandwidth is 100 Mbps.
The Dual Stack Network: AWS is one of the CSPs to offer IPv6 support natively.
Upgrades and Patching: Operating System needs patching at the kernel and application level. The patches are periodically done by unattended upgrades, which is handled by an application.
Domain Name Registration: The domain name "team-h.ml" has been registered to suit. Glue records are the means to attach our nameservers at the registrar so that we would be able to act as Name Server, but only for acting as Authoritative Name Server.
The Server Software Installation: Server software is one of the prime software that has the capability to answer client's queries. Considering the NGINX application, BIND9 application is packaged and is available at major Linux-based distributions. Both server software have been installed and security measures have been considered even during installation.

Subdomain decisions for various uses: subdomains for offering services.

DoH - dns.team-h.ml
DoT - dot.team-h.ml
DoQ - doq.team-h.ml
Elliptic Curve Cryptography (ECC) and getting signed by a trusted CA: ECC is very fast when compared to the RSA algorithm. It has smaller key sizes and thus introduces lower overheads when compared to the RSA algorithm.
subject=CN = doq.team-h.ml
issuer=C = US, O = Let's Encrypt, CN = R3

subject=CN = dns.team-h.ml
issuer=C = US, O = Let's Encrypt, CN = R3
subject=CN = dot.team-h.ml
issuer=C = US, O = Let's Encrypt, CN = R3

Planning for Cipher Suites and TLS versions that promote PFS: Cipher Suites are the key components in TLS.
Supported Server Cipher(s): Table 1 and Table 2

Table-1: Supported Server Ciphers

TLS Version	Length	CipherSuite
TLSv1.3	128 bits	TLS_AES_128_GCM_SHA256
TLSv1.3	256 bits	TLS_AES_256_GCM_SHA384
TLSv1.3	256 bits	TLS_CHACHA20_POLY1305_SHA256
TLSv1.2	128 bits	ECDHE-ECDSA-AES128-GCM-SHA256
TLSv1.2	256 bits	ECDHE-ECDSA-AES256-GCM-SHA384
TLSv1.2	256 bits	ECDHE-ECDSA-CHACHA20-POLY1305

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910015 |

Table-2:Server Key Exchange Groups		
TLS Version	Length	ECDH Curve
TLSv1.3	128 bits	secp256r1 (NIST P-256)
TLSv1.3	192 bits	secp384r1 (NIST P-384)
TLSv1.3	260 bits	secp384r1 (NIST P-384)
TLSv1.3	128 bits	x25519
TLSv1.2	192 bits	secp256r1 (NIST P-256)
TLSv1.2	260 bits	secp384r1 (NIST P-384)
TLSv1.2	128 bits	secp384r1 (NIST P-384)

V. RESULTS AND DISCUSSION

After deployment proceed to do the security and transport protocol tests. Test is conducted is in the early stages in standardization of the protocol QUIC, the results might have varying values.

The Name Server lookup:

The lookup done on our domain names evaluates to the IP Addresses. This shows that the **doh.team-h.ml** &**doq.team-h.ml** are directly pointing to the origin servers, whereas the **dns.team-h.ml** is pointing to the CDN.

$ host dns.team-h.ml
dns.team-h.ml has address 104.21.94.127
dns.team-h.ml has address 172.67.135.252
dns.team-h.ml has IPv6 address 2606:4700:3035::6815:5e7f
dns.team-h.ml has IPv6 address 2606:4700:3036::ac43:87fc

$ host dot.team-h.ml
dot.team-h.ml has address 52.66.195.98
dot.team-h.ml has address 13.234.18.191
dot.team-h.ml has IPv6 address 2406: da1a:c8: b200::15
dot.team-h.ml has IPv6 address 2406: da1a: d19:3d02:18af: b81c: e462:79f8

$ host doq.team-h.ml
doq.team-h.ml has address 13.234.18.191
doq.team-h.ml has address 52.66.195.98
doq.team-h.ml has IPv6 address 2406: da1a: d19:3d02:18af: b81c: e462:79f8
doq.team-h.ml has IPv6 address 2406: da1a:c8: b200::15

The DoH test over HTTP/2 and HTTP/3 (experimental):

The figure 4 shows the support of QUIC and HTTP/3 protocols which are tested by a site hosted by LiteSpeed. The test has been done on our servers and also on the CDN PoP. The testing server was successfully able to establish the QUIC connection and transfer application data over HTTP/3. There is a support for 0-RTT achieved using QUIC as a transport protocol. The subversions for HTTP/3 which have been proved to be supported are

H3-27 - HTTP/3 Draft version 27
H3-28 - HTTP/3 Draft version 28
H3-29 - HTTP/3 Draft version 29

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910015 |

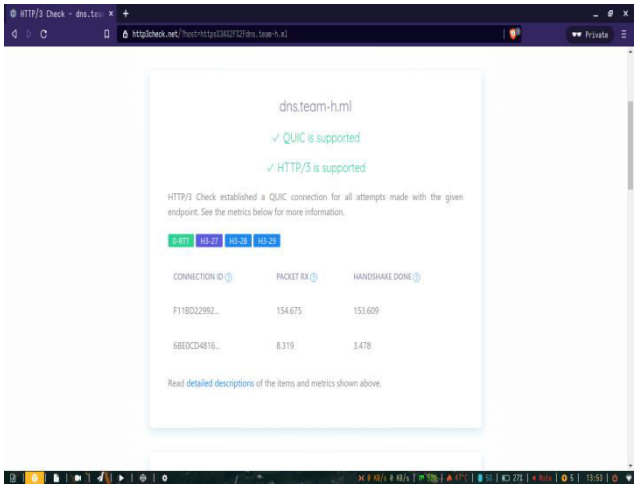

FIG-4 HTTP/3 AND QUIC SUPPORT

The above versions have been implemented by most of the experimental servers and clients. Hence our servers support the protocol versions.
Considering the client side, the below are the results achieved and proves the support for various protocols like DoH, DoT, DoQ (experimental).

Once it is up, the DNS sample lookup should happen in such a way that it uses **10.154.65.49 (in our case)** as a DNS Resolver. Hence, on doing so,

```
; <<>> DiG 9.16.15 <<>> zappy.wtf @10.154.65.49
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57791
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;zappy.wtf.                     IN      A

;; ANSWER SECTION:
zappy.wtf.              274     IN      A       15.206.111.111

;; Query time: 51 msec
;; SERVER: 10.154.65.49#53(10.154.65.49)
;; WHEN: Tue May 18 12:27:51 IST 2021
;; MSG SIZE  rcvd: 54
```

FIG-5 DNS SAMPLE LOOKUP

Also note that the CDN at this stage is using HTTP/1.1, because it is considered optimal when compared to HTTP/2. HTTP/2 is not suitable for backend servers.

Domain Blocking section:

The below are some of the rules present in our RPZ Database. The test proves that our servers are capable of performing RPZ operations.

```
zyrtec.4.p2l.info IN CNAME.
zytpirwai.net IN CNAME.
zytrox.tk IN CNAME.
```

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910015 |

```
zyzlk.com IN CNAME.
zz.690tx.com IN CNAME.
zz.cqcounter.com IN CNAME.
zzhc.vnet.cn IN CNAME.
zzz.clickbank.net IN CNAME.
zzz.onion.pet IN CNAME.
zzzrtrcm2.com IN CNAME.
```

VI. CONCLUSION

We have successfully implemented one of the futuristic protocols to the Domain Name System. Successfully created a working model that makes use of the defined protocols, thus ensuring faster performance and security. The proposed system will help the users of the different network to do their basic resolution activities. The security features that come with QUIC enable secure delivery of the content. Hence, proposed model that fits in the Open Source world.

REFERENCES

[1] Ramaswamy Chandramouli, (NIST) Scott Rose and (NIST), "Secure Domain Name System (DNS) Deployment Guide," September 2013.
[2] C.Huitema, A.Mankin and S.Dickinson, “Specification of DNS over Dedicated QUIC Connections draft-ietf-dprive-dnsoquic-00,” 27 April 2020. (https://datatracker.ietf.org/doc/html/draft-ietf-dprive-dnsoquic-00).
[3] C.Huitema, A.Mankin and S.Dickinson, “Specification of DNS over Dedicated QUIC Connections draft-ietf-dprive-dnsoquic-00,” 20 October 2020. (https://datatracker.ietf.org/doc/html/draft-ietf-dprive-dnsoquic-01).
[4] C.Huitema, A.Mankin and S.Dickinson, “Specification of DNS over Dedicated QUIC Connections draft-ietf-dprive-dnsoquic-02,” 22 February 2021. (https://datatracker.ietf.org/doc/html/draft-ietf-dprive-dnsoquic-02).
[5] Manjunath CR, “Layer Based Secure Data Aggregation for Wireless Sensor Network”, International Journal Of Engineering And Computer Science(IJECS) ISSN:2319-7242 Volume 3 Issue 6, June 2014
[6] Manjunath CR, “Hop-by-Hop Message Authentication Based on Block Cipher Approach in Wireless Sensor Networks”, International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015), Vol. 3, Issue 3 (July - Sept. 2015), ISSN : 2347 - 8446 (Online) ISSN : 2347 - 9817 (Print), pp 25 – 27
[7] Manjunath CR, “Security of Smart Objects in IoT”, International Journal of Innovative Technology and Research IJITR, ISSN 2320-5547, pp 128 – 130, 2015
[8] Manjunath CR, **“**Cyber Attacks and Counter Measures – A Survey**”,** International Journal of Applied Engineering Research, ISSN 0973-4562 Vol. 10 No.86 (2015), Research India Publications pp 313 – 319
[9] Manjunath CR, “Multicast routing for mesh-based using DSR in wireless sensor network”, International Journal of Engineering & Technology, 7 (3.29) (2018) 173-176
[10] Manjunath CR, “A Study on Recent Trends and Developments in Intrusion Detection System”, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 11, Issue 6 (May. - Jun. 2013), PP 27-30, ISSN: 2278-8727
[11] Manjunath CR, “Secure Transmission in MANET and Wireless Sensor Network” International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE), ISSN (Print): 2320 – 3765, ISSN (Online): 2278 – 8875, Vol. 3, Issue 5, May 2014.
[12] Manjunath CR, “A Survey: Energy Efficient Routing Techniques in Mobile Wireless Sensor Network”, International Journal of Computer Science Trends and Technology (IJCST) – Volume 3 Issue 4, Jul-Aug 2015, ISSN: 2347-8578, pp 223 – 227
[13] “NGINX-build by our team”. (https://github.com/zap51/nginx-quic-bin).
[14] “Let's Encrypt is a free, automated, and open certificate authority brought to you by the nonprofit Internet Security Research Group (ISRG)”. (https://letsencrypt.org/).
[15] “Stub Resolver written in Python”. (https://github.com/zap51/stub-doh-bin).[8] "A simple DNS proxy server that supports all existing DNS protocols including DNS-over-TLS, DNS-over-HTTPS, DNSCrypt, and DNS-over-QUIC. Moreover, it can work as a DNS-over-HTTPS, DNS-over-TLS or DNS-over-QUIC server". (https://github.com/AdguardTeam/dnsproxy)

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details