DNS over TLS and HTTPS

Chandana Ramesh
18307309
rameshc@tcd.ie

June 4, 2019

1 Introduction

The chapter aims to signify the prevalent idea about Domain Name System (DNS) and will narrow down the prime research motive. A distributed database containing mappings of domain names to data is also a protocol for Transmission Control Protocol or Internet protocol (TCP/IP) network. The DNS deals with increasing number of Internet users around the world, enabling users to use friendly, hierarchical names to find computers on a network. It translates names like www.dot.com, into Internet Protocol (IP) addresses, such as 160.153.137.14 (or extended IPv6 addresses), thus, assisting computers to communicate with each other. It acts as a medium to access Internet applications, such as the World Wide Web (www) easily. DNS defines the following:

- Method to query and update the database
- Mechanism to reproduce information in the database between servers
- Database schema

2 Overview

The Stanford Research Institute - Network Information Centre (SRI-NIC) was initially the sole responsible body store unique host names on the Internet. A single text file named hosts.txt was used and websites updated SRI-NIC regularly with the IP address and domain name mappings. Managing this list turned into a challenge with the rapidly growing Internet. Furthermore, each host names are required to be unique worldwide. With the accelerated growth in Internet usage, it became impractical to assure the distinctive host names. It was the need for a distributed and hierarchical naming structure that acted as a foundation for the introduction of a network protocol that could scale globally leading to the creation of a distributed database that mapped host names to their respective IP address, called DNS. Using a distributed database also enforced that no organisation would be solely responsible but rather moved the control to organisations managing their host names.

2.1 Fundamentals

The DNS resolves host names to IP address called forward resolution and address to host name knows as inverse resolution. The DNS has emerged as an important element of Internet due its distributed characteristics and robustness in mapping human memorable name to numerical address. Since accessing resources using IP addresses is not an efficient method, DNS is densely relied on to retrieve addresses by using Fully Qualified Domain Name (FQDN).

2.1.1 Domain Name Space

The end dot represents the root domain of the Internet's name space. DNS names are labelled corresponding to a node thus, recognising each node uniquely. A FQDN represents the path long the tree structure to the root domain, commonly referred as the root zone. The left section of the FQDN represents the host name while the right section represents the local domain to which the host is a part of. The local domain may be a subdomain of a different domain. As the tree is traversed from the root to the leaf nodes, the nodes become most specific. Fig shows an example of a FQDN.

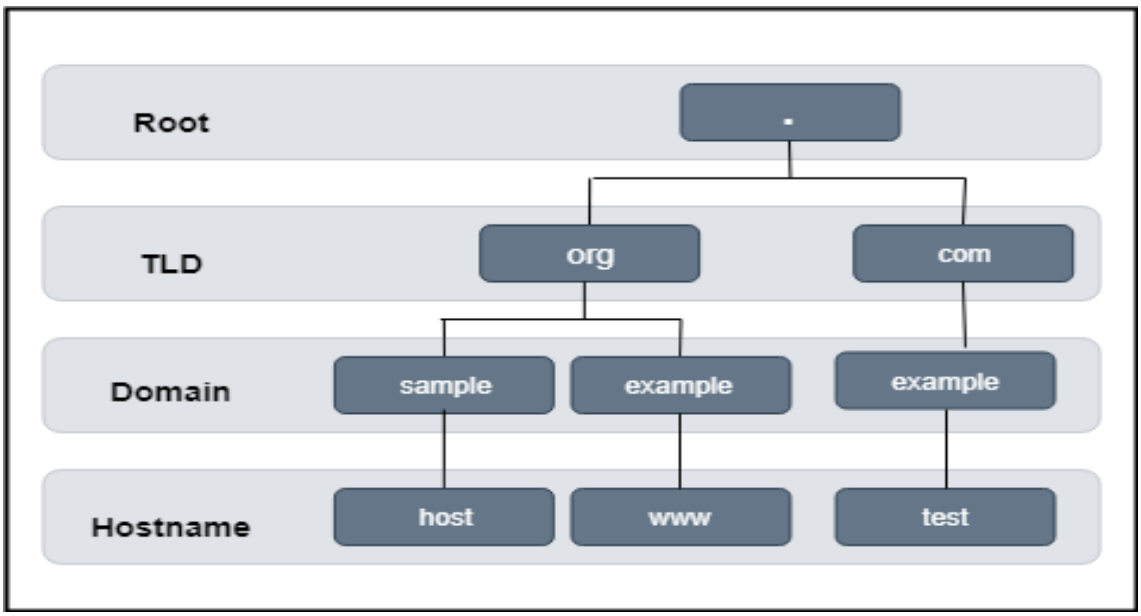

Figure 1: "Forward Lookup"

When DNS uses inverse resolution, it uses labels right to left i.e. from most specific to the least for defining IP address which contrast to the common description of IP address whose decimal notation if from least to most specific (left to right). For this purpose, the IP addresses of DNS is always represented in reverse order. IP addresses belong to Top Level Domain (TLD) which is known as in-addr.arpa. ¡INSERT IMAGE¿

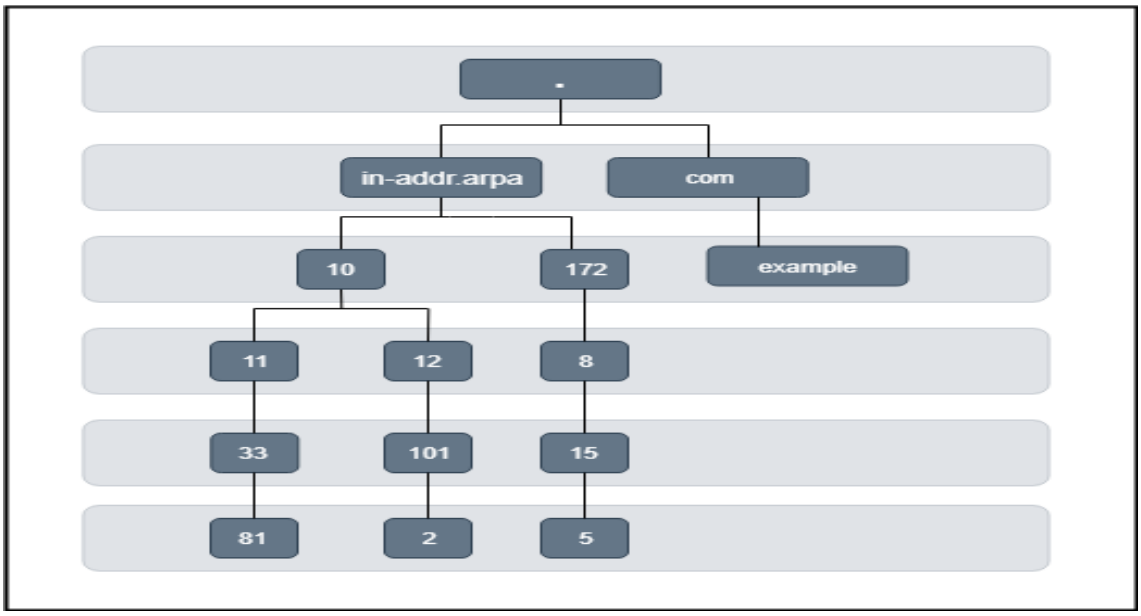

Figure 2: "Forward Lookup"

2.1.2 Components

Domain Name Servers have the following components Database, a distributed database containing Name Space and Resource Records (RRs) defining names within the name space. Name servers manage a portion of the name space and aid in discovering hostnames or addresses inside a tree.

Name servers act as delegation points in determining other servers that hold authority over subdomains. Zone information is the RR data that are discovered on the name servers making up the domain. Each zone can either be forward or reverse depending on whether it returns information of a domain or maps addresses to host names respectively. Changes made to data in a zone is recorded in the primary server. Secondary name servers contain copies of primary server database. There are a total of 6 fields in a RR namely, TYPE, NAME, CLASS, RD Length, TTL and RDATA ¡Is it necessary to define each type?¿. Common Resource Records are shown in ¡INSERT TABLE¿

Multiple Resource Records are grouped into sets (RRSets) consisting of 0 or more RRs having similar DNS class, name and type but different data. Clients contain functions responsible for obtaining information from the name space on behalf of the application. Such functions are packaged together into a library, known as the resolver library therefore, the clients are known as resolvers. The main functions of the resolver library is querying the name server for information involving a DNS record and sending the reply back to the resolver.

3 Research Motivation

¡Use this as Introduction to Motivation¿ Over the past many years, attackers have hijacked domain names to manipulate and redirect users to malicious sites. Consider for example, a user trying to access a service portal, redirected to a website that seems legitimate. This compromises the user's credentials through an authentication form or sometimes card payment details. The Gandi incident in 2017 is an example of a large-scale distribution attack wherein, the attacker gained access to a huge number of domain names of which 751 websites were compromised including modification of name servers to alter traffic flow to malicious sites exploiting security weakness in many browsers. Transport Layer Security, a cryptographic protocol is used to secure the traffic flow and communication in the world wide web. Since most of DNS queries are transferred as clear text, anyone will be able to sniff and gather information. DNS was formerly functioning on UDP as a stateless mode which made it more liable to IP address spoofing leading to impersonating server and sending forged queries. Since UDP does not support many encryption fixes, it becomes complicated.

3.1 Public Nature of DNS queries

DNS queries are transmitted unenrypted and have least confidentiality concern. DNS publicly maintains records about domain names and the corresponding IP addresses. However, the hosts accessing this data is assuredly non-public. But, this information may easily be available to other entities like organizations, government etc. by eavesdropping. The data that is revealed could provide information like a person's email, contact, chat and more.

3.2 DNS requests

As part of privacy concerns, the source IP address and QNAME are two particularly important fields which may reveal information about the user's actions. Consider an example of a query containing host part as www.security.com of type A and requesting MX records for the domain. These types of requests disclose transmission relation [3]. Due to the lack of privacy it becomes risky to introduce personally identifiable, sensitive data in DNS and becomes a foremost concern if MUA's explore PGP keys.

3.3 Network Channels

Like any other traffic and since DNS queries are made in clear text, the traffic may be available by eavesdroppers. The DNS traffic may flow through recursive and authoritative name servers and not just between the sender and the receiver hence the access points are wider in case the direct channel is not available to tap. Since the medium between recursive and stub resolver is not restricted by caching, it is the convenient surface to tap.

4 Related Work

There has been minimum work carried out to provide privacy between a client and a server. DNSSEC presents response integrity by using cryptographic signatures on zones permitting end users to validate if the replies are right. However, DNSSEC fails to preserve privacy of request and response. Other work includes DNSCrypt, DNSCurve, IPSECA and Confidential DNS.

The DNS traffic may leak information about the activity of a user on the internet giving away details of the email services they are using or the software the user is running. Repressive regimes may record activities of citizens browsing the internet, for example, look for users who resolve the name of a VPN server by an external organization which may help dissidents exchange information with the outside world.

5 Attack Types

Many companies do not realise that DNS is an important attack point and it is the most overlooked com-

ponent. This section lists the common types of attacks:

5.1 Domain Hijacking

This kind of attack exploits the exposure of registrars system involving alterations to the registrar and domain name servers that deviate the traffic from the original path to another destination. Once this is done, the attacker instigates malicious tasks like setting up a payment method, stealing personal data that are critical by creating an identical copy of the original site.

5.2 DNS Flood Attack

Flood attack is one of the most common types of attack on DNS and is carried out by overloading the server till it cannot serve any more DNS queries since the all RR's are affected by the DNS zones. This case worsens if it turns out to be a Distributed Denial Service (DDoS) involving multiple hosts. Although, it is instantly detectable, it makes many lawful requests thereby confusing the defence systems making the mitigation harder.

5.3 Distributed Reflection Denial of Service

DDoS aims at making the target inaccessible by denying access to the system while DRDoS is slightly different and more successful. It involves sending requests to its servers and spoofs the source address causing systems to reply and flood the destination. This is usually initiated by programmed botnets to amplify the effect of the attack.

5.4 Cache Poisoning

Also known as spoofing, is a well known and one of the most common attack types. The hijacker will identify the vulnerabilities in the system and exploit it by introducing malevolent content in the victim's resolver cache, redirecting the affected user to another server. Once this is successful, attackers receive legal data to their servers and steal information from visitors.

5.5 DNS Tunelling

To be successful in carrying out this type of attack, attackers need access to compromised authoritative, DNS server and the domain name and additionally control an authoritative server. A request is sent by a user which includes encoded hostname and domain name. The data payload is added to the attackers DNS server and consequently gains control over remote server. Other types of attacks include DNS hijacking, NXDOMAIN, Random subdomain and Phantom domain attacks.

6 Implementation

File /etc/hosts is used for small networks whose contents are not altered frequently. It is a basic method for resolution of domain name to IP addresses. Any web machine can be reached using its name, alias or IP address. However, for address resolution in large networks, using /etc/hosts file is insufficient and a devoted service for this purpose should be used. The Domain Name Server commissions the authority of designating names and mapping these to resources on the Internet by allocating authoritative name servers for every domain. The DNS defines the detailed functionality of database service which forms its foundation and describes the protocol that is a comprehensive specification of data communication and structures included as part of the Internet Protocol Suite.

6.1 BIND

For DNS server installation and configuration, I used Berkeley Internet Name Daemon (BIND) and related utilities. Named.conf file is where the instructions for recursive caching server is present. We create forward and reverse zone for each of the domains that are defined in separate files. !!WRITE MORE

6.2 Debugging

- Dig - Since we used the dnsutil package, we test the configuration by using dig, which is a DNS lookup service.
- Ping - sends an ICMP request to show how hostname is resolved by an application.

- Named-checkzone – installed along with the bind9 package is used to test is the configuration of the zone files before bind9 utility is restarted. It outputs an OK indicating success else lists the errors.
- Logging – Bind9 can be set up to send debug and error messages associated with DNS queries to a dedicated file.