LGURJCSIT
Volume No. 1, Issue No. 3 (July- September), pp. 50-59

Infrastructure of DNS/DNSSEC

Zaka Ullah
Department of Computer Science
Lahore Garrison University

Abstract: - DNS Security Extension is introduced as a solution after the in-depth study of all expected issues regarding security of Domain Name System. Accordingly, DNS is domain name service provider via name server but it fails to facilitate with the support for authenticity of data origin and integrity. In addition, DNS satirizing give stage to digital assaults, and can be used to watch client's exercises, for control, for conveyance of pernicious programming and to offend client's PC and even to subvert rightness and accessibility of internet systems and administrations. Therefore, it is fundamental to attract DNS framework to defeat security concerns, and to make cautious arrangement that should adapt to assaults through off way foes. So, we have broken down security of area enlistment centers and name server completely and we deal with vulnerabilities, which should open DNS foundation to store harming. In this paper, we gave the DNSSEC structure and showed how it is secure using DNSSEC.

1. Background: -

The Domain Name System is use in the web naming administrations. DNS is real asset for correspondence of web applications. These applications generally keep running over TCP/IP based corporate online worlds, for example, web perusing, email, CRM, ERP, Active Directory and others.

The present security apprehension with DNS that is also the main cause of dissatisfaction is the phishing assault that basically utilizes DNS reserve harming to take touchy budgetary data. This issue of DNS security is settled by utilizing DNSSEC that gives information honesty and inception verification utilizing irregular key and HMAC-MD5.

In this paper, we objectified DNSSEC and sent DNSSEC quickly, we may fight off a disastrous bargain of the Internet's DNS foundation.

2. DNS Infrastructure

DNS translates domain names to IP addresses, and vice versa. DNS is implemented as a globally distributed database supporting a hierarchical structure[1]. A customer substance known as a Resolver follows up for a customer by submitting questions to, and accepting reactions from, the DNS server. The reactions contain Resource Records (RRs) containing the coveted name/address determination information. The

accessibility and execution of DNS is improved through a replication and reserving mechanism [1]. Essentially DNS is the customer/server correspondence, DNS customers send demand to and get reactions from DNS servers.

Demand containing a name that outcomes in an IP address being come back from the server, are called forward DNS queries.

Requests containing an IP address and resulting in a name, called *reverse DNS lookups,* are also supported. DNS implements a distributed database to store this name and last-known address information for all public hosts on the Internet[2]. The DNS name space is composed progressively. An area is a sub tree of the name space. The top-level areas (TLDs) are those promptly beneath the root. An area is broken into littler units called zones.

2.1 Name Server and Resolver

Resolver is essentially a customer and it sends the demand to the recursive server and get some information about a specific zone in a zone record. A name server may reserve data about any piece of the space tree, yet when all is said is done it has finished data about a particular piece of the DNS. This means the name server has authority for that subdomain of the name space - therefore it will be called *authoritative*[3]. Recursive or reserve forwarder are mindful that concentrate the data from name servers in light of customer ask.

2.2 DNS Query Resolutions

Basically, naming server works in two modes, one is recursive and second is called iterative. Resolver send to inquiry to recursive with RD (Recursion Desired) signal set on in the DNS question header. Recursive server finds through the DNS progression in light of inquiries and return however never exchange to the name server. Iterative inquiries work by the iterative server counsel its own database for the asked information. On the off chance that it can't get the appropriate response, it gives the IP address of the nearest name server that may know the outcome. The resolver rehashes the demand, this time sending it to the server it spared the known data. As a matter, of course questions go to root name server are iterative.

2.3 DNS Working Flow

Figure 1 demonstrates the arrangement of DNS inquiry and answer messages.

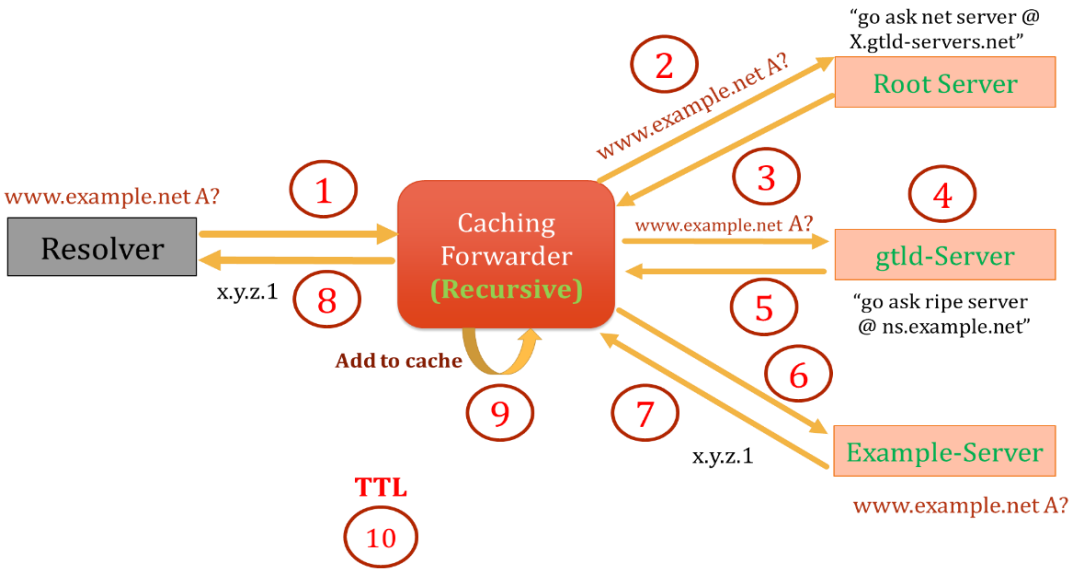

Figure 1: Arrangement of DNS

2.4 DNS Tree

Essentially DNS is tree structure, it has diverse levels. The root is situated at the top and is spoken to by dot. The following level is called Top Level Domain (TLD) allotted by InterNIC. The hub Labels utilized can be up to 63 octets long each, albeit every one of the names altogether should not surpass 255 octets. The **Fully Qualified Domain Name (FQDN)** is a list of these labels with the labels nearest the root listed on the right of the full name [4].

The root has the saved 'Zero Length' name it has spoken to by '.', however the names are case sensitive and we can't have a similar name for another branch at a similar level yet we can utilize a similar mark on an alternate branch of the tree. The 2 top-most used types of TLDs are the generic TLDs such as the domains.com,.net,.edu and.org, as well as country-code TLDs whose last name suffix refers to country specific sites such as.nl for the Netherlands, .uk for Great-Britain, etc. [5]. These TLD-servers once again refer to the next layer which is generally authoritative for that domain name and returns the requested mapping**[5]**.

2.5 Resource Record

Name server have asset records in zone documents, particularly, the RR comprises of the accompanying significant fields:

- Name: Pointer to the RR.
- TTL: Time to live the time allotment that a stored RR might be thought to be legitimate.

- Class: its type of network; RRS typically belong to the IN (Web) class.
- RRType: type of resource

Most regular RRTypes are:

- A: Address RRType. A RR of this sort gives the IP deliver to a host name (recognized utilizing a FQDN). **[6]**
- MX: Mail Exchanger RRType. A RR of this sort gives the mail server have name for a domain. [6]
- NS: Name Server RRType. A RR of this sort gives a name server have name for a domain. [6]

3. DNS Vulnerabilities

We now briefly survey the absolute most vital assaults on DNS. A large portion of these issues have been already recorded.

3.1 Man in the middle (MITM) attacks:

Domain name server has no legitimate method for confirming its beginning or checking its trustworthiness. This is the main reason DNS does not stipulate a component for servers to give validation detail for the information they forward to customers. A resolver has no strategy to confirm the credibility and respectability of the information sent by name servers. The Resolver can just validate the starting point of a DNS answer information bundle utilizing the source IP address of the DNS server, goal and source port numbers and DNS exchange ID. Man in the center assaults can without much of a stretch took a DNS server reaction bundle to coordinate these parameters. The customer has no arrangement yet to trust as dependable the information given by an assailant. An aggressor can resolve true blue inquiries, reacting with false data.

3.1.1 Packet Sniffing

Essentially DNS sends a question or reaction in a solitary unsigned, decoded UDP parcels, which are effectively alter. While catching DNS question parcels, at that point produced the wrong answer and forward to the resolver. Resolver never thinks about the aggressor catch the DNS answer parcel from the name server and alter it. It has no source to check the validation or information honesty.

3.1.2 Transaction ID Predicting

An attacker can answer with false responses to a figure question, without being on the LAN to capture parcels. Store forwarder will answer either by the resolver or by the reserving name server. The DNS exchange ID field is just a 16-bit field, and the server UDP port related with DNS is 53. On the customer, there are just 2^{32} conceivable mixes of ID (2^{16}) and customer UDP ports (2^{16}) for a given customer and server. Practically speaking the customer UDP port and the Exchange ID can be anticipated from past questions.

It is regular for the customer port to be a known settled an incentive because of firewall confinements, or the port number will increase incrementally due to resolver library conduct. The DNS exchange ID produced by a customer normally increases incrementally. This diminishes the pursuit space to a range littler than 2^{16} [7]. Without anyone else, ID speculating is insufficient to enable an assailant to infuse sham information. This must be consolidated with information or suppositions about Questions (QNAME) and Inquiry sort (QTYPE) for which a resolver may be questioning. This can, for instance, be accomplished by reserve snooping [8].

3.2 Caching Problems

Recursive or cache forwarder are mindful in answering the inquiry of resolver. In the event that recursive or reserve forwarder is trade off, at that point attacker can without much of a stretch adjust the DNS information. The current DNS convention does not bolster any way to proliferate information updates or nullifications to DNS servers or reserves in a quick and secure way.

3.2.1 Cache Poisoning using Name Chaining

The attacker infuses false data into DNS caches. The principle goal of interloper is DNS asset record whose RDATA divide incorporates a DNS name which can be utilized as a snare to give an attacker a chance to nourish information into a casualty's reserve. The most imperative piece of RRs is CNAME, NS, and DNAME RRs. Alter information related with these names, can be infused into the casualty's cache by means of the extra area of the reaction. An interloper can present subjective DNS names of the attacker's picking, and give additional data that is asserted to be related with those names.

3.2.2 Cache Poisoning using Transaction ID Prediction

In this attack, most of resolution request are sent to the victim server (ns1.hbl.com, say) with spoofed source IP addresses to resolve a name, say www.hbl.com. Every request has own unique transaction ID and processed independently. Since ns1.hbl.com is attempting to determine each of these solicitations, the server will be anticipating an extensive number of answers from ns1.hbl.com. The attacker utilizes the holdup stage to attack ns1.hbl.com with mock answers from ns1.hbl.com, expressing that www.hbl.com focuses to an IP address which is under the aggressor's control. Each mock answer has an alternate exchange ID, a source port and the ridiculed DNS server IP address (for ns1.hbl.com). The interloper plans to figure the right exchange ID and source port utilized by the questioning name server. Once the assault is effective, false data will be put away in the recursive server.

3.3 Other major DNS attacks

3.3.1 Information Leakage

Some time zone exchange by an aggressor would go to as an examination assault, perhaps uncovering delicate data about outer system arrangement, e.g. the IP locations of outer firewall interfaces. DNS names could, for instance, speak to extend names that might be of regard for an assailant, or could uncover the personality of the OS running on the machine.

3.3.2 DNS Dynamic Update Vulnerabilities

Dynamic Host Configuration Protocol (DHCP) is use in the DNS Dynamic refresh convention to include and erase asset records request. These updates occur on the essential server of the zone [9]. Those such updates are given validation is construct solely with respect to source IP address, and is helpless against danger, for example, IP ridiculing. These assaults can go from dissent of administration, including erasure of records, to redirection [10].

4. Domain Name System Security Extensions (DNSSEC)

DNSSEC remain for Area Name Administration Security Augmentations. Its redesign form of DNS and ensures against such assaults by carefully "marking" information so we are certain that it is legitimate. In any case, on the off chance that we have to take out the defenselessness from the web, it must be sent at each progression in the query from root zone to conclusive space name (e.g. www.dfrsc.org). Sending DNSSEC on the root zone is a vital stride in the general procedure. Regularly it doesn't encode information. Just bears witness to the legitimacy of the address of the site we visit. For DNSSEC the quality of each connection in the chain of trust depends on the trust the client has in the association reviewing key and different DNS data for that connection [11]. Keeping in mind the end goal to ensure the uprightness of this data and save this trust once the information has been confirmed it must be quickly shielded from mistakes, regardless of whether malignant or coincidental, which can be presented at whatever time key information is traded crosswise over hierarchical boundaries [11].

4.1 DNSSEC Keys (KSK and ZSK)

KSK remains for Key Signing key (a long value key) and ZSK remains for Zone Signing Key (a here and now key) [11]. Given adequate time and information, cryptographic keys can inevitably be traded off. On account of the asymmetric or open key cryptography utilized as a part of DNSSEC, this implies an attacker decides, through savage constrain or different techniques, the private portion of people in

general private key match used to make the marks verifying the legitimacy of DNS records [11].

This enables him to vanquish the securities managed by DNSSEC. DNSSEC ruins these trade off endeavors by utilizing a transient key – the zone marking key (ZSK) – to routinely register marks for the DNS records and a long haul key – the key marking key (KSK) – to figure a mark on the ZSK to enable it to be approved [11].

The ZSK is changed or moved over every now and again to make it troublesome for the attacker to "figure" while the more KSK is changed over an any longer era (current accepted procedures put in this on the request of a year). Since the KSK signs the ZSK and the ZSK signs the DNS records, just the KSK is required to approve a DNS record in the zone. It is an example of the KSK, as a Delegation Signer (DS) record that is left behind to the "parent" zone. The parent zone (e.g. the root) signs the DS record of the youngster (e.g.,. organization) with their own particular ZSK that is marked by their own KSK [11].

4.2 Transaction Signature (TSIG)

Transaction signatures (TSIG) is an instrument used to secure DNS messages and to give secure server-to-server correspondence (generally amongst ace and slave server, however can be stretched out for dynamic updates also) [12]. TSIG can protect the following type of transactions between two DNS servers:

- Zone transfer
- Notify
- Dynamic updates
- Recursive query messages etc

TSIG is available for BIND v8.2 and above. TSIG uses shared secrets and a one-way hash function to authenticate DNS messages. TSIG is easy and lightweight for resolvers and named. [12]

5. Conclusion

DNS is associated with multiple security issues that should be resolved urgently. Because of inaccessibility of realness and respectability in the DNS exchange handle, we experience different dangers like reserve harming. Support flood can occur due to insuitable and nonexistent limit checking and blunder dealing with conditions. Misconfigured customer resolvers to parcel channels causing conditions are principle reasons that prompt utilization dangers. The Internet Engineering Task Force (IETF) has encourage to defeat dangers through creating DNSSEC convention i.e. secure, keeps up information respectability and resolves DNS store harming. DNSSEC provides transaction level authenticity and

gives safe zone transfers by securing all data within zone during transfer. In short DNSSEC successfully trace outs Name based attacks.

References

[1] S. Ariyapperuma and C. J. Mitchell, "Security vulnerabilities in DNS and DNSSEC," *Proc. - Second Int. Conf. Availability, Reliab. Secur. ARES 2007*, pp. 335–342, 2007.

[2] DNS(Domain Name Services) How DNS Works https://www.lifewire.com/definition-of-domain-name-system-816295

[3] A. Lioy, F. Maino, M. Marian, I. Politecnico, and T. Torino, "DNS Security," *Informatica*, pp. 1–13, 2000.

[4] Domain Name System (DNS) The DNS Tree http://www.rhyshaden.com/dns.htm

[5] N. L. M. Van Adrichem, A. R. Lua, X. Wang, M. Wasif, F. Fatturrahman, and F. A. Kuipers, "DNSSEC misconfigurations: How incorrectly configured security leads to unreachability," *Proc. - 2014 IEEE Jt. Intell. Secur. Informatics Conf. JISIC 2014*, pp. 9–16, 2014.

[6] R. Chandramouli and S. Rose, "Secure Domain Name System (DNS) Deployment Guide," 2013.

[7] D. Atkins and R. Austein. Threat analysis of the domain name system (DNS). RFC 3833, Internet Engineering Task Force, Aug. 2004.

[8] L. Grangeia. Dns cache snooping. Technical report, Security Team —Beyond Security, February 2004.

[9] P. Vixie, S. Thomson, Y. Rekhter, and J. Bound. Dynamic updates in the domain name system (DNS UPDATE). RFC 2136, Internet Engineering Task Force, Apr. 1997.

[10] D. E. 3rd. Secure Domain Name System dynamic update. RFC 2137, Internet Engineering Task Force, Apr. 1997.

[11] DNSSEC, Important for DNSSEC security https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-en

[12] Bind Security: (Transaction Signatures (TSIG) Configuration) https://www.cyberciti.biz/faq/unix-linux-bind-named-configuring-tsig/