DNS Best Practices, Network Protections, and Attack Identification

Overview

This white paper provides information on general best practices, network protections, and attack identification techniques that operators and administrators can use for implementations of the Domain Name System (DNS) protocol.

What is DNS?

DNS is a globally distributed, scalable, hierarchical, and dynamic database that provides a mapping between hostnames, IP addresses (both IPv4 and IPv6), text records, mail exchange information (MX records), name server information (NS records), and security key information defined in Resource Records (RRs).

The information defined in RRs is grouped into zones and maintained locally on a DNS server so it can be retrieved globally through the distributed DNS architecture. DNS can use either the User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) and historically uses a destination port of 53. When the DNS protocol uses UDP as the transport, it has the ability to deal with UDP retransmission and sequencing.

DNS is composed of a hierarchical domain name space that contains a tree-like data structure of linked domain names (nodes). Domain name space uses Resource Records (RRs) that may or may not exist to store information about the domain. The tree-like data structure for the domain name space starts at the root zone ".", which is the top most level of the DNS hierarchy.

Although it is not typically displayed in user applications, the DNS root is represented as a trailing dot in a fully qualified domain name (FQDN). For example, the right-most dot in "*www.cisco.com.*" represents the root zone. From the root zone, the DNS hierarchy is then split into sub-domain (branches) zones.

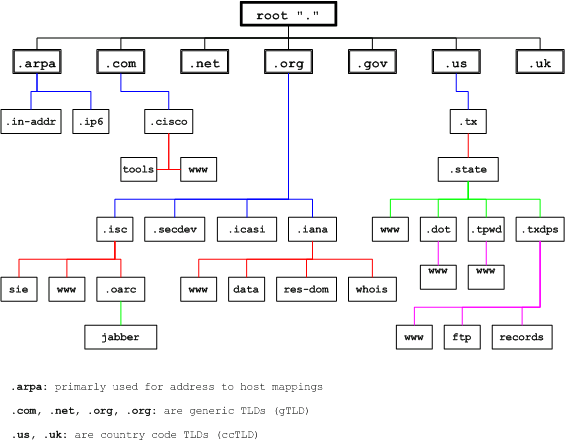
Each domain name is composed of one or more labels. Labels are separated with "." and may contain a maximum of 63 characters. A FQDN may contain a maximum of 255 characters, including the ".". Labels are constructed from right to left, where the label at the far right is the top level domain (TLD) for the domain name. The following example shows how to identify the TLD for a domain name:

**com** is the TLD for **www.cisco.com** as it is the label furthest to the right.

**Domain Name Space**

The following diagram illustrates a sample of the Domain Name System hierarchy starting from the root "**.**". Everything below the "**.org**" domain name space is in the *org* domain and everything below "**.cisco.com**" domain name space is in the *cisco.com* domain.

**Figure 1. Domain Name Space**



The DNS protocol specification and implementation was originally defined in [RFC 882](http://tools.ietf.org/html/rfc882) and [RFC 883](http://tools.ietf.org/html/rfc883).

These RFCs were made obsolete by [RFC 1034](http://tools.ietf.org/html/rfc1034) and [RFC 1035](http://tools.ietf.org/html/rfc1035) and have been updated by multiple RFCs over the years.

**Important DNS Terminology**

To understand DNS and the DNS-specific recommendations in this document, it is important that operators and administrators are familiar with the following terms:

* **Resolver:**A DNS client that sends DNS messages to obtain information about the requested domain name space.
* **Recursion:**The action taken when a DNS server is asked to query on behalf of a DNS resolver.
* **Authoritative Server:**A DNS server that responds to query messages with information stored in RRs for a domain name space stored on the server.
* **Recursive Resolver:**A DNS server that recursively queries for the information asked in the DNS query.
* **FQDN:**A Fully Qualified Domain Name is the absolute name of a device within the distributed DNS database.
* **RR:**A Resource Record is a format used in DNS messages that is composed of the following fields: NAME, TYPE, CLASS, TTL, RDLENGTH, and RDATA.
* **Zone:**A database that contains information about the domain name space stored on an authoritative server.

**Primary Function of DNS**

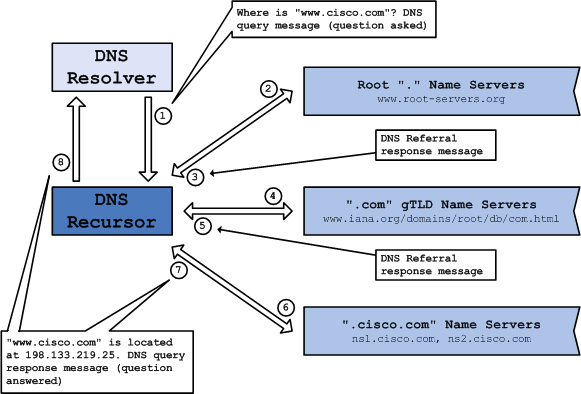
DNS primarily translates hostnames to IP addresses or IP addresses to hostnames. This translation process is accomplished by a DNS resolver (this could be a client application such as a web browser or an e-mail client, or a DNS application such as BIND) sending a DNS query to a DNS server requesting the information defined in a RR.

Some examples of the DNS resolution process follow:

* If the DNS server is only configured as an authoritative server and it receives a DNS query message asking about information which the server is authoritative, it will cause the server to inspect locally stored RR information and return the value of the record in the 'Answer Section' of a DNS response message. If the requested information for the DNS query message does not exist, the DNS server will respond with a NXDOMAIN (Non-Existent Domain) DNS response message or a DNS Referral Response message.
* If the DNS server is authoritative, not configured as a recursive resolver, and it receives a DNS query message asking about information which the server is not authoritative, it will cause the server to issue a DNS response message containing RRs in the 'Authority Section' and the address mapping for the FQDN from that section may be present in the 'Additional Section'. This informs the DNS resolver where to send queries in order to obtain authoritative information for the question in the DNS query. This is also known as a DNS Referral Response message.
* If the DNS server is not authoritative but is configured as a recursive resolver and it receives a DNS query asking about information, it will cause the server to recursively query (iterative queries) the DNS architecture for the authoritative DNS server of the information included in the DNS request. Once the recursive DNS resolver has obtained this information, it will provide that information to the original DNS resolver using a DNS response message and the RR will be non-authoritative (since the recursive DNS resolver is not authoritative for the requested information). The recursive DNS resolver may also have knowledge about the requested information stored in DNS cache. If the requested information is present in the DNS cache, then the recursive DNS resolver will respond with that RR information.

Figure 2 illustrates the iterative process used by a DNS recursive resolver (DNS Recursor, server) to answer the DNS query message (question) on behalf of the DNS resolver (DNS Resolver, client) and provide a DNS query response message (answer).

**Figure 2. Recursive Query**



1. The DNS resolver sends a query message to the recursive resolver asking for the address of [www.cisco.com](http://www.cisco.com/).
2. The DNS recursor sends a query message to the root name servers looking for the *.com* domain name space.
3. The root name servers send a DNS referral response message to the DNS recursor informing it to ask the gTLD name servers for the *.com* domain name space.
4. The DNS recursor sends a query message to the gTLD name servers looking for the *.cisco.com* domain name space.
5. The gTLD name servers send a DNS referral response message to the DNS recursor informing it to ask the *.cisco.com* name servers, *ns1.cisco.com* or *ns2.cisco.com*, about this domain name space.
6. The DNS recursor sends a query to*ns1.cisco.com* or *ns2.cisco.com* asking for [www.cisco.com](http://www.cisco.com/).
7. The *.cisco.com* name servers, *ns1.cisco.com* or *ns2.cisco.com*, send an authoritative DNS query response message to the DNS recursor with the A (address) RR information for www.cisco.com.
8. The DNS recursor sends a DNS query response message to the DNS resolver with the A (address) RR information for [www.cisco.com](http://www.cisco.com/).

**DNS Messages**

All legitimate DNS messages sent or received are composed of multiple sections. These sections of the DNS message contain fields that determine how the message will be processed by the device receiving the message. These sections also contain information about the question (query messages) a device is asking or answers (response messages) a device may be providing. The sections present in a DNS message are Header, Question, Answer, Authority, and Additional.

Note that there are situations where sections of the DNS message may be empty. An example is a 'DNS Referral Response Message', in which the Answer section is empty, but the Authority and Additional sections are present and contain RR information.

For more information about the sections of a DNS message, their format, and the fields they contain, consult [RFC 1035](http://tools.ietf.org/html/rfc1035), Section 4., Messages.

Maliciously Abusing Implementation Flaws in DNS

Flaws in the implementation of the DNS protocol allow it to be exploited and used for malicious activities. Because DNS is such a critical protocol for Internet operations, countless operating systems, and applications, operators and administrators must harden DNS servers to prevent them from being used maliciously. Some of these flaws are presented in this document to inform operators how they can be used maliciously. Techniques are shared that can be used to prevent these types of activities.

**DNS Open Resolvers**

A DNS open resolver is a DNS server that allows DNS clients that are not part of its administrative domain to use that server for performing recursive name resolution. Essentially, a DNS open resolver provides responses (answers) to queries (questions) from anyone asking a question. DNS open resolvers are vulnerable to multiple malicious activities, including the following:

* DNS cache poisoning attacks
* DNS cache poisoning attacks‡
* Resource utilization attacks

‡Denial of Service (DoS) or Distributed DoS (DDoS)

**DNS Cache Poisoning Attacks**

DNS cache poisoning occurs when an attacker sends falsified and usually spoofed RR information to a DNS resolver. Once the DNS resolver receives the falsified RR information, it is stored in the DNS cache for the lifetime (Time To Live [TTL]) set in the RR. To exploit this flaw in the DNS resolver implementation so it will store the falsified information, an attacker must be able to correctly predict the DNS transaction identifier (TXID) and the UDP source port for the DNS query (request) message. Attackers use this exploitation technique to redirect users from legitimate sites to malicious sites or to inform the DNS resolver to use a malicious name server (NS) that is providing RR information used for malicious activities.

**DNS Amplification and Reflection Attacks**

DNS amplification and reflection attacks use DNS open resolvers to increase the volume of attacks and to hide the true source of an attack, actions that typically result in a DoS or DDoS attack. These attacks are possible because the open resolver will respond to queries from anyone asking a question. Attackers use these DNS open resolvers for malicious activities by sending DNS messages to the open resolvers using a forged source IP address that is the target for the attack. When the open resolvers receive the spoofed DNS query messages, they respond by sending DNS response messages to the target address. Attacks of these types use multiple DNS open resolvers so the effects on the target devices are magnified.

**Resource Utilization Attacks**

Resource utilization attacks on DNS open resolvers consume resources on the device. Examples of such resources include CPU, memory, and socket buffers. These types of attacks try to consume all available resources to negatively impact operations of the open resolver. The impact of these attacks may require the device to be rebooted or a service to be stopped and restarted.