World Wide Web (DNS)

Hostnames:

– IP address for computers (32/128 bit) (containing routing information)

* Name e.g. [www.yahoo.com](http://www.yahoo.com) – used by humans

Domain Name Systems:

* Service that translates host name to IP address
* Found on application layer
* A distributed database implemented in hierarchy of many name servers
* An application layer protocol that allows hosts to communicate with name servers to resolve names (address/name translation)
* DNS is commonly employed by other application layer protocols such as for example HTTP and FTP to translate user-supplied hostnames to IP addresses.
* EXAMPLE: When for example a browser (HTTP client) requests URL, www.bbc.co.uk, the following is happening:
  + - i. Host runs the client side of the DNS application
    - ii.Browser extracts the hostname www.bbc.co.uk from the URL and passes the hostname to the client side of the DNS application
    - iii. DNS client send a query containing the hostname to a DNS server
    - iv. DNS client receives a reply containing the translation
    - v. Browser receives the IP address and open a TCP connection with the Web server [www.bbc.co.uk](http://www.bbc.co.uk)

DNS Services:

* Host aliasing: long host names can be shortened to mnemonic host names. Long name is called canonical name (CNAME).
* Mail server Aliasing: same as above for emails
* Load Distribution: load balancing. Multiple (replicated) servers working on the same page but with different IP addresses

DNS Distributed Database - There is one primary server for a domain, and typically a number of secondary servers containing replicated databases. This is true in all levels of hierarchy

Hierarchical Database:

* 1. Host contact local DNS
* 2. Local DNS send the query to a root DNS
* 3. Root DNS returns a list of TLD DNS for the .edu domain
* 4. Local DNS resends to a TLD DNS local DNS server
* 5. TLD DNS returns IP address of the authoritative DNS server
* 6. Local DNS re-sends query to the authoritative DNS dns.poly.edu
* 7. Authoritative DNS returns IP address
* 8. Local DNS reply with the requested IP address of gaia.cs.umass.edu
  + Recursive – asking another agent to optain mapping for you
  + Interative – fetching all quieres for itself
* Uses Caching and negative caching.

DNS Resource Records: {Name, Value, Type, TTL}

A – Map a hostname to an IP address ● NS – Which Name Server is authoritative for a domain ● CNAME - “Canonical Name” used to make one domain an alias of another ● MX - “Mail Exchange” a list of mail exchange servers

TYPE A:

Tutorial

1. When an attacker attempts to insert a fake address record into the DNS. After a poisoning, subsequent requests will be controlled by the attacker.
2. Authoritative DNS server - contains local servers e.g. “amazon.com” etc…., Top level domain server – contains the “. co.uk”, “.com” “.edu” servers , Root DNS server – Top level in the hierarchy, 13 worldwide
3. Client will type in hostname into URL bar, this is then converted to IP address by DNS server and then is queired by Root level server, TLD and authoritative servers then eventually shows webpage to client
4. A DNS Resource Record (RR) is the unit of information entry in **DNS** files; RRs are the basic building blocks of host-name and IP information and are used to resolve all **DNS** queries.
5. A RR is compliled of a question section and a answer section. The question section has infor about the query that is being made by the DNS server and the Answer section contains the reply to the query being asked above. Each RR will have a Type {A, NS, CNAME MX}, a value and TTL (Time to leave – Time spent in Cache)