CS 456 Hao Pan
Salahuddin, Mohammad
Spring 2018

Chapter 2.4 DNS (Domain Name System)

05/06/2018 [T]

2.4.1 Overview

- People have many identifiers. They have their *names*, their *social security number*, their *passport*... So do network devices.
- Internet hosts and routers use a *32 bit IP address* for addressing datagrams.
- The *"name"*, its url, is used by humans.
- **DNS** is used to map between IP address and name.
  - It is a *distributed database* implemented in a hierarchy of many namer servers.
  - *Application-layer protcols* such as *hosts* and *name servers* communicate to *resolve* names.

2.4.2 DNS Services and Structure

2.4.2.1 DNS Services

- Hostname to IP address translation.
- Host aliasing.
- Mail server aliasing.
- Load distribution (multiple IP addresses could correspond to one name).

2.4.2.2 DNS Structure

- See slide 2-63 for example of a DNS hierarchy.
- Client queries must start at the root DNS server and work their way down to the right DNS server to get the right IP address.
- Local name servers contact **root name servers** if they cannot resolve a name. The root name server will contact an *authoritative name server* if they don't know the name server either. The mapping, once acquired, is returned to the local name server.
- **Top Level Down**, or *TLD* servers are responsible for domains such as *com, org, net, edu...* as well as top-level country domains like *uk, fr, ca, jp....*
- **Authoritative** DNS servers provide mappings only for hosts within an organization.
- **Local DNS name servers** do not belong strictly in a hierarchy.
  - Every ISP usually has one, including companies and universities.
  - When the host makes a query, the query is sent to its local DNS server, which has a cache of recent mappings stored locally. They act as a proxy and forward the query into the hierarchy.

- There are 2 methods for DNS name resolution:
  - **Iterated query**, when the contacted server replies with the name of the server to contact instead.
  - **Recursive query**, when the burden of the name resolution is passed onto the contacted name server.
- Once a name server learns a mapping, it will *cache* that mapping - though the cache entry will eventually *time out (TTL)*.
- Cached entries may be *out-of-date*, so if the name host's IP address changes, the new IP address will not be known until the TTLs expire.

2.4.3 DBS Records

- DNS records are stored in the following *resource records (RR)* format: **(name, value, type, ttl)**.
- The entries represent different things for different **types**:
  - **type=A**:
    - **name** is the hostname.
    - **value** is the IP address.
  - **type=NS**:
    - **name** is the domain (ex. foo.com).
    - **value** is the hostname of the authoritative name server of the current domain.
  - **type=CNAME**:
    - **name** is the alias name for the canonical real name.
    - **value** is the canonical name.
  - **type=MS**:
    - **value** is the name of the mailserver associated with the name.

2.4.4 DNS Protocol Messages

- *Queries* and *replies* both have the same message format.
- A visual example can be seen on slide 2-71.
- **Identification**: a 16-bit number is used for the query. Replies use the same number.
- **Flag** states whether:
  - The message is query or reply.
  - Recursion is desired.
  - Recursion is available.
  - Reply is authoritative.
- The message body contains 32-bit sections for:
  - Name and type fields for a query.
  - RRs in response to the query.
  - Records for authoritative servers.
  - Additional possibly helpful information.

2.4.5 Inserting Records into DNS

- To insert a new record into DNS, the name must be registered at the **DNS registrar**.
- The name and IP addresses of authoritative name servers must be provided.
- Two RRs will be placed into the corresponding TLD server: One is *NS*, and one is *A*.
- See slide 2-73 for an example.

2.4.6 Attacking DNS

- DDoS attacks:
  - The root servers are bombarded with traffic, which isn't very successful because traffic is filtered, and local DNS servers cache IPs which enable them to bypass the root server.
  - If the TLD servers are bombarded, it is potentially more dangerous.
- Redirect attacks:
  - Man-in-middle, where queries are intercepted.
  - DNS poisoning, when bogus replies are sent to the DNS servers to cache.
- Exploit DNS for DDoS, when queries with spoofed source addresses are sent to the target IP.