DNS Protocol and Attacks

An interesting story related to DNS

In the 2004 presidential debate between John Edward and the vice president Dick Cheney, Cheney said the following: "Well, the reason they keep mentioning Halliburton is because they're trying to throw up a smokescreen. They know the charges are false. They know that if you go, for example, to **FactCheck.com**, an independent Web site sponsored by the University of Pennsylvania, you can get the specific details with respect to Halliburton".

The debate was broadcasted live on TV. Within a few minutes, the web site of **FactCheck.com** received a tremendous amount of traffic. Unfortunately for Cheney, the actual web site should be **FactCheck.org**, a politically neutral web size, not FactCheck.com. George Soro, who does not like President Bush, immediately capitalized on this mistake by somehow (he might paid the owner of FactCheck.com for doing so) redirecting all the FackCheck.com bound traffic to his own web site, where the top item is an article by Soros entitled "Why we must not Re-Elect President Bush".

1 DNS (Domain Name Service)

- Motivation
  - Human prefer pronounceable names rather numeric IP addresses
  - Machines prefer numeric IP addresses
  - We need to have a mechanism to translate the pronounceable names to IP addresses, so the machines can understand.
- Original Naming Scheme: flat structure.
  - The original names formed a flat namespace without structure, A central site, the Network Information Center (NIC), administered the namespace. Later, the NIC was replaced by the INTERnet Network Information Center.
  - Advantage: names are convenient and short
  - Disadvantage: a flat namespace cannot generalize to large sets of machines for both technical and administrative reasons.
    - Potential conflict
    - Names are assigned by a center server
    - Maintaining correct copies of the entire list at each site is difficult
- Hierarchical Names
  - Decentralizing the naming mechanism: delegating authority and distributing responsibility
  - A hierarchical naming scheme works like the management of a large organization.
    - The namespace is partitioned at the top level

    - The authority for names in subdivisions is passed to designated agents

- DNS
  - Specifies the name syntax and rules for delegating authority over names
  - Specifies the implementation of distributed computing system that efficiently map names to addresses.
- DNS Syntax
  - Set of labels separated by delimiter character (period)
  - Example: `ecs.syr.edu`
  - `syr.edu` is also a domain
  - The top-level domain is `edu`
- Mapping Domain Names to Addresses
  - Name server: supplies name-to-address translation
  - Client: uses one or more name servers when translating a name
  - DNS uses a set of on-line servers
  - Servers arranged in tree
  - A given server can handle entire subtree. For example, a sever at ECS manages the domain names within the `ecs.syr.edu` domain.
- Type of DNS queries
  - Recursive: often used by the client
  - Iterative: often used by the local DNS server
- Recursive query and Iterative query:
  - A resolver sends a recursive query to a name server for information about a particular domain name. The queried name server is then obliged to respond with the requested data or with an error stating that data of the requested type don't exist or that the domain name specified doesn't exist.
  - If the queried name server isn't authoritative for the data requested, it will have to query other name servers to find the answer. It could send recursive queries to those name servers, thereby obliging them to find the answer and return it (and passing the buck). Or it could send iterative queries and possibly be referred to other name servers "closer" to the domain name it's looking for. Current implementations are polite and do the latter, following the referrals until an answer is found.
- DNS caching: After the local DNS server obtains the query results from another DNS server, it will store the results in its cache for certain period of time. The timeout duration can be spcified in the DNS response.
- An example of DNS query process: The process is straightforward. Here's one example in which a local name server uses iterative queries to resolve an address for a client:

1. The local name server receives a name resolution request from a client system for a host name (such as www.google.com).
2. The local name server checks its records. If it finds the address, it returns it to the client. If no address is found, the local name server proceeds to the next step.
3. The local name server sends an iterative request to the root (the "." in .com) name server.
4. The root name server provides the local name server with the address for the top-level domain (.com, .net, etc.) server.
5. The local name server sends an iterative query to the top-level domain server.
6. The top-level domain server replies with the IP address of the name server that manages the host name's domain (such as google.com).
7. The local name server sends an iterative request to the host name's domain name server.
8. The host name's domain name server provides the IP address for the host name (www.google.com) being sought.
9. The local name server passes that IP address to the client.

- Inverse Mappings
  - Implemented by a separate, parallel tree, keyed by IP address.
  - `222.33.44.3` $\Rightarrow$ `3.44.33.222.in-addr.arpa`
  - The Internet root domain servers maintain a database of valid IP addresses along with information about domain name servers that can resolve each address.
- DNS Port
  - The DNS uses TCP and UDP on port 53 to serve requests.
  - Almost all DNS queries consist of a single UDP request from the client followed by a single UDP reply from the server.
  - TCP typically comes into play only when the response data size exceeds 512 bytes, or for such tasks as zone transfer.
- DNS response: here is a sample DNS response.

```
;; QUERY SECTION:
;;      syr.edu, type = A, class = IN

;; ANSWER SECTION:
syr.edu.                1D IN A         128.230.18.35

;; AUTHORITY SECTION:
syr.edu.                1D IN NS        icarus.syr.edu.
syr.edu.                1D IN NS        lurch.cns.syr.edu.
syr.edu.                1D IN NS        suec1.syr.edu.

;; ADDITIONAL SECTION:
lurch.cns.syr.edu.      1D IN A         128.230.12.5
suec1.syr.edu.          1D IN A         209.164.131.32
```

```
icarus.syr.edu.         1D IN A         128.230.1.49

;; Total query time: 1 msec
;; FROM: nyx to SERVER: default -- 128.230.12.5
;; WHEN: Tue Feb  2 22:23:22 2010
;; MSG SIZE  sent: 25  rcvd: 154
```

  - AUTHORITY SECTION contains NS records pointing to name servers closer to the target name in the naming hierarchy. This field is completely optional, but clients are encouraged to cache this information if further requests may be made in the same name hierarchy.
  - ADDITIONAL SECTION contains records that the name server believes may be useful to the client. The most common use for this field is to supply A (address) records for the name servers listed in the Authority section.

- DNS software
  - BIND (Berkeley Internet Name Domain): DNS server
  - Microsoft DNS (in the server editions of Windows 2000 and Windows 2003)
  - The `dig` command (DNS client): dig = "domain information groper".

2 DNS Root Servers, Top-Level Domains, and Registration

- DNS Root Servers
  - There are 13 DNS root servers from `A.ROOT-SERVERS.NET`, `B.ROOT-SERVERS.NET` to `M.ROOT-SERVERS.NET`.
  - These root servers have well known IP addresses, and should be used when configuring DNS servers. For example, the A servers IP address is `198.41.0.4`, operated by VeriSign and the B servers IP address is `192.5.5.241`, operated by ISC, etc. The IP addresses of these servers can be obtained from `http://www.internic.net/zones/named.root`.
  - Currently (2007), 6 of the 13 root servers are not single machines. They represent several physical servers each in multiple geographical locations. For example, The F rootserver answers queries over IPv4 on `192.5.5.241`, and over IPv6 on `2001:500::1035`. Service for this sever is provided by a distributed collection of nameserver nodes located in many places, using a Hierarchical Anycast technique running ISC BIND 9.
    - See `www.root-servers.org` to see where thehse root servers are.
  - Until mid-2000, the root servers also handled all requests for the generic top level domains. Due to the potential denial of service attacks, this responsibility was later removed from the root servers and led to the creation of dedicated Top-Level Domain Servers to handle .com, net, .org, country code, etc.
  - The root servers' zone file is published at `http://www.internic.net/zones/root.zone`. A company can run its own root server within the company, as long as it can synchronize with the published zone file. This way, its DNS servers do not need to go to the external root servers.

- Top-Level Domains (TLDs)

  - Original TLDs:
    * Generic TLDs (gTLDs): EDU, COM, NET, ORG, GOV, MIL, and INT
    * Country-code TLDs (ccTLDs): .FR (France), .CN (China), .IN (India), etc.
  - Lift of restrictions on TLDs:
    * On June 20, 2011 the ICANN board voted to end most restrictions on the names of generic top-level domains (gTLD). Companies and organizations will be able to choose essentially arbitrary top level Internet domain names.
    * ICANN will begin accepting applications for new gTLDS on January 12, 2012.
    * The initial price to apply for a new gTLD will be $185,000.
    * The renewal or the annual fee of the domain will further be $25,000.
  - Who is in charge: The Internet Assigned Numbers Authority (IANA) is responsible for the overall coordination and management of the Domain Name System (DNS), and especially the delegation of TLDs. IANA is operated by the Internet Corporation for Assigned Names and Numbers (ICANN).

- Domain Name Registration

  - **Registry**: Each TLD is delegated by IANA to a "designated manager", called *registry*, which maintains the database of names registered within the TLD it administers. The major concern in selecting a designated manager for a domain is that it be able to carry out the necessary responsibilities, and have the ability to do a equitable, just, honest, and competent job. There is a strict protocol and policies that governs the selection of designated managers (RFC 1591). IANA reserves the right to revoke and to redelegate a TLD to another manager if there are misconducts by the current manager.
    * VeriSign is the designated manager for two of the important TLDs: `.COM` and `.NET`.
    * EDUCASE is the designated manager for `.EDU`.
  - **Registrar**: Domain name registries contract with domain registrars to provide registration services to the public. An end user selects a registrar to provide the registration service, and that registrar becomes the designated registrar for the domain chosen by the user.
    * Go Daddy is the largest registrars currently.
    * They also offer other related services to customers.
  - **Registrants**: The registrants (users of a domain name) are customers of the registrar, in some cases through additional layers of resellers.

3 Attacking DNS Protocols

- Denial of Service attacks against DNS servers.

  - May 19th 2009: an attack on the servers of a domain registrar in China caused an online video application to cripple Internet access in parts of the country late on Wednesday. This was caused by a chain effect:
    * Several DNS servers of DNSPod (a Chinese domain service provider and registrar) were hit by a DDOS attack on the night of May 18. These DNS servers became inaccessible.

    - The assault was meant to be a targeted attack against one company, but one of the customers of DNSPod is Baofeng.com, whose authoritative DNS server was the server under attack. Baofeng is a widely popular media player in China, with a total of 200 million users and several million users online simultaneously.
    - Because of a design flaw in Baofengs media player, all online Baofeng programs started continuously sending DNS queries, after the DNS responses previously cached by other servers timed out on May 19.
    - The massive number of DNS queries flooded the network of China Telecom (one of the biggest ISPs in China). As a result, users in parts of China were unable to access websites.
    - Internet users in more than 20 provinces were affected on May 19, the ministry said. It was described as the worst Internet incident in China, with nearly 300 million users, only after a service interruption due to damaged undersea cables during an earthquake near Taiwan on December 26, 2006.
    - Internet access returned to normal several hours later. But the incident caused wide calls in China for increasing safety measures of Internet.
    - Baofeng company Monday announced it would recall 120 million online video playing software whose faulty design was believed to have automatically caused continuous requests on the server.
    - DNS is part of the Internet infrastructure that many people depend on. Although the above unintended Baofeng incident is probably rare (due to a software bug), it demonstrates how vulnerable the Internet is when its major pieces, DNS servers, are under attack.
  - December 24th 2009: In a sudden Denial-of-Service attack on DNS provider to Internet's major e-commerce companies, UltraDNS suffered an outage for an hour. The DoS attack on UltraDNS was felt by thousands of online shoppers in Northern California. The attack hit Amazon.com, resulting in slowdowns and outages. It also hit some of the other sites like Walmart.com, Gap.com, Second Life (Linden Labs), Salesforce.com, SomaFM.com, and Expedia.com.

- Unrelated Data Attack
  - To improve performance, DNS servers can send back more information than what the client has asked for. For example, if the client asks for the IP address of `www.mysite.com`, the DNS server can also send back the IP addresses for `ftp.mysite.com` and `mail.mysite.com` to avoid another likely DNS lookup.
  - In the older version of DNS servers, the validity of the extra information is not verified. The actual information does not even need to be related to the original query. Therefore, a malicious DNS server from `mysite.com` can send back the faked IP addresses for `Citibank.com`, tricking users to go to the malicious site when they try to connect to Citibank.

```
;; ANSWER SECTION:
www.syr.edu.              1D IN A         128.230.18.20
www.example.edu.          1D IN A         128.230.18.35
```

  - This problem has been fixed in BIND, by forbidding anything that is not related to the original request to be cached.

- Related Data Attack
  - The process is the same as the unrelated data attack

  - The hacker has to make the extra information related to the original query
    * MX: mail server for a domain
    * CNAME: canonical name for an alias
    * NS: DNS servers for a domain
  - The above information is "related" to the original request, but they can point to totally different information the hacker wants to be cached.

```
;; AUTHORITY SECTION:
syr.edu.                1D IN NS    www.example.com.
;; ADDITIONAL SECTION:
www.example.com.      1D IN A       128.230.18.35
```

  - The problem has also been fixed in BIND, by rejecting all the "out of zone" information. In the above example, the `www.example.com` is beyond the zone of `syr.edu`, so its IP address mapping will be rejected.

- Reverse DNS attacks
  - Assume `nyx.syr.edu` and `apollo.syr.edu` trust each other, and the trust is based on name, not the IP address.
  - Also assume that you are from `hacker.com`, and you have the control of your own DNS server.
  - How can you exploit the trust relationship between `nyx` and `apollo`?
    * When `nyx` receives a connection from an IP address, it needs to use the reverse DNS lookup to find out the hostname of the IP address.
    * The reverse lookup will start from the root, then goes to `arpa.in-addr`, and eventually goes to the DNS server of the owner of the IP address. If the IP address is the attacker's machine, the query will go to the DNS server of `hacker.com`, which will tell you anything that they want, including saying that the IP address's hostname is `apollo.syr.edu`.
  - Q: How to prevent this?
    * Use IP address for the trust relationship
    * A second (forward) DNS look up.

- DNS Pharming Attacks: aiming to redirect a websites traffic to another, bogus website. Many techniques can be used, and mostly target DNS. Details of Pharming attacks can be found from our DNS attack lab.
  - Insider attack: corrupted insiders can modify the local DNS servers to mislead users to bogus websites.
  - Corrupted hosts: if a host is already corrupted, there are many things attackers can do to affect the DNS. Users of the corrupted machines can go to bogus websites when they visit their favorite sites. Here are some popluar tactics by attackers:
    * Modify the `/etc/hosts` file in Unix systems.
    * Modify Windows Hosts file to map specific domain names to specific IP addresses.
    * Modify Windows registry settings to reference specific (rogue) DNS servers.
    * Create a scheduled task under Mac OS X to reference specific (rogue) DNS servers

    * Exploit cross-site request forgery vulnerabilities in routers to overwrite the DNS server configuration offered to local area network clients.
- DHCP attack: Serving the rogue DNS server configuration over DHCP, the protocol responsible for distributing dynamic IP addresses, as well as other information, including DNS settings.
- Domain Registration Attacks: when a domain registration expires and the owner forgot to renew it, attackers can buy that domain legally and hijack the domain. Attackers can also buy the domain names that are similar to their targets. If users misspell the domain names, they might become victims.
- Corrupting DNS servers. Change the mappings on the corrupted DNS servers.
- DNS cache Poisoning.
    * Victim DNS server asks other DNS servers for mappings if it doesn't have them. It then caches the mappings.
    * DNS cache poisoning is to poison the clients cache.
- DNS Spoofing: Answer DNS queries intended for another server. There are several challenges:
    * **Timing:** DNS spoofing must be conducted after the victim sends out a DNS query. How can attackers time that? There are many methods: (1) Attackers can send a request to the victim DNS server, asking it to get a mapping for a domain name; since that is the job of the DNS server, a DNS query will be sent out upon receiving the request. (2) If a firewall prevents the external attackers from sending DNS request to the victim DNS server within the firewall's boundary, the attackers can trick an inside user from initiating the DNS request. For example, the attacker can send emails to an inside user, and ask them to click the URL of the target domain; this way, an DNS request will be sent out by the user. As long as the attackers is informed of this click (not difficult to achieve), they can time the DNS request.
    * **Transaction ID (16 bits):** each DNS query contains a random 16-bit transaction ID. Replies must carry this ID.
    * **Source UDP port (16 bits):** in some operating systems, the source UDP port is also a 16-bit random number.
    * **Local or Remote attacks:** If the attacker is on the same network as the victim, the attacker can observe the traffic, and thus obtain the transaction ID and the source UDP port. However, if the attacker is remote, sniffing the information becomes infeasbile.
    * **Cache effect:** For remote attackers, guessing the correct source ports and transaction ID is necessary. However, if the guessing is incorrect, the spoofed reply will lose to the legitimate reply. Because the reply will be cached for a while, the attackers cannot make another guess until the cached DNS mapping times out.
    * **Dan Kaminsky Attack:** An elegant attack that bypass the cache effect. The idea is not to send a request for `www.example.com` if your target is `www.example.com`. Instead, send `a.example.com`, `b.example.com`, ... In the spoofed reply, attach the IP address for `www.example.com` in the *additional field*. This way, if the spoofed replies lose to the legitimate replies, the IP address for `www.example.com` will not be cached, because the IP address is unlikely to be included in the legitimate replies. Therefore, the attackers can keep trying, until its own spoofed replies beat the legitimate replies. As long as the attackers' chance of winning the race is not zero, sooner or later, the attackers will succeed.

4 DNSSEC

- DNSSEC (short for DNS Security Extensions) adds security to the Domain Name System.
- DNSSEC is a set of extensions to DNS, which provide: (a) origin authentication of DNS data, (b) data integrity, and (c) authenticated denial of existence.
- DNSSEC requires the modification of the DNS protocol.
- The root zone will be DNSSEC signed in July 2010.
- `http://ispcolumn.isoc.org/2006-08/dnssec.html`
- `http://www.cs.ucla.edu/~eoster/doc/todsc-paper.pdf`