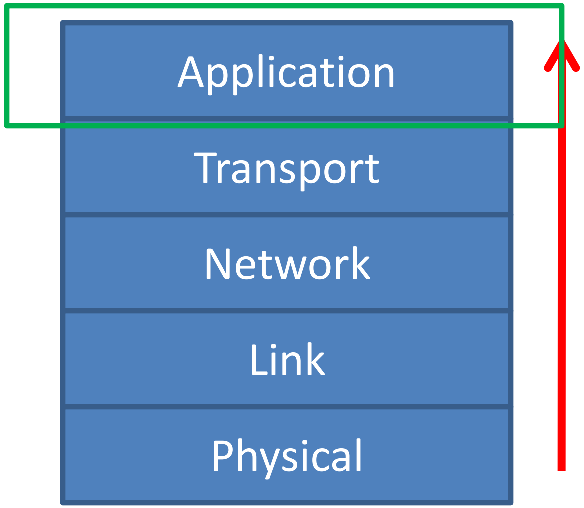
Computer and Network Security: Network Attacks

Kameswari Chebrolu

Outline

- Attacks at different layers of the protocol stack
- Solutions to the same



Application Layer Role

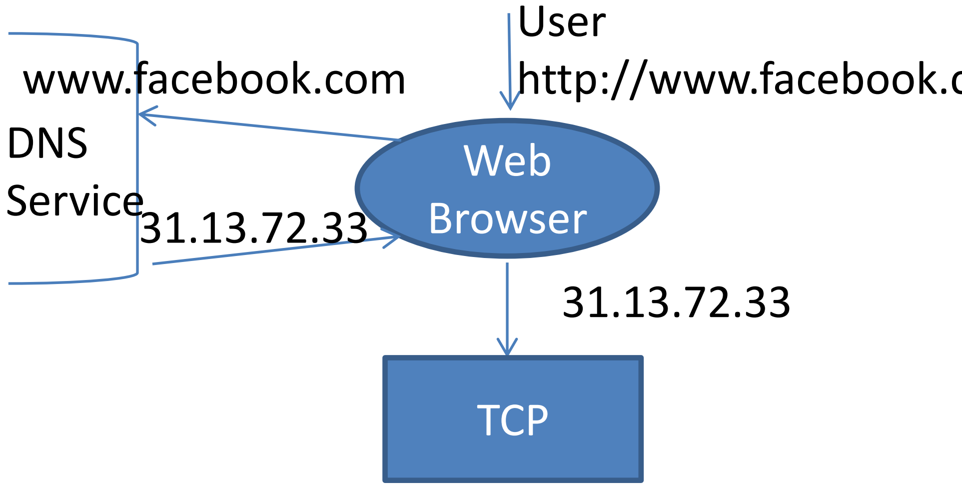
- Network infrastructure in place to enable variety of applications
  - Can transfer packets from a process on a given host to another process on another host
- Role of application developers:
  - Develop interesting/useful applications
  - Understand the building blocks and their interaction
  - Make the right choices and implement required functionality

Application Protocols

Application	Protocol	Transport
E-mail	SMTP (RFC 2821)	TCP
Remote terminal access	Telnet (RFC 854)	TCP
Web	HTTP (RFC 2616)	TCP
File Transfer	FTP (RFC 959)	TCP
Streaming Multimedia	Proprietary	TCP or UDP
Internet Telephony	Proprietary	Often UDP
Domain Name System	**DNS**	**UDP**

DNS: Problem and Solution

- People prefer hostnames
- Routers prefer IP addresses
- Need a service (DNS) that converts hostnames/domains to <u>Values</u>

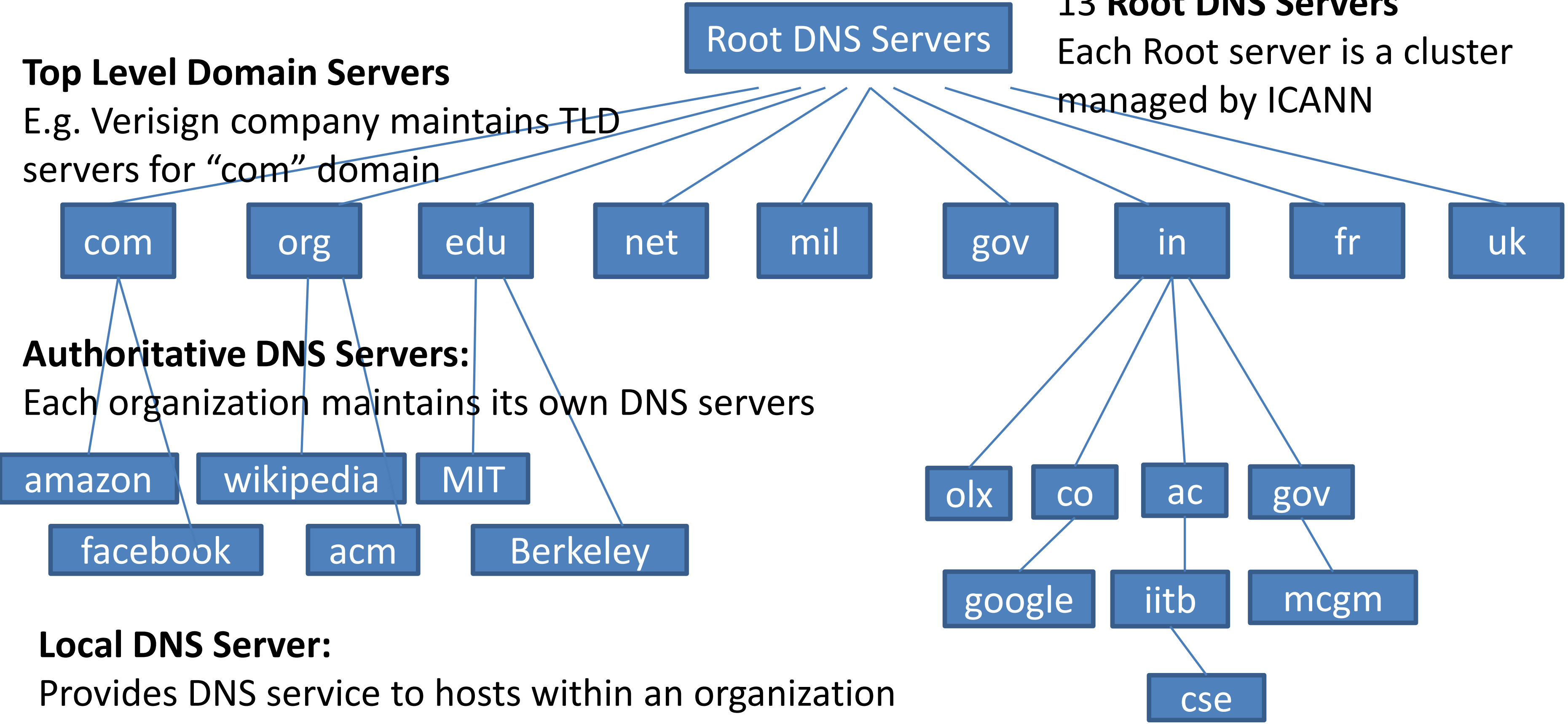


Domain Name: Label that defines a realm of administrative autonomy
E.g. facebook.com; iitb.ac.in; mit.edu

Hierarchical and Distributed Implementation

13 **Root DNS Servers**
Each Root server is a cluster managed by ICANN

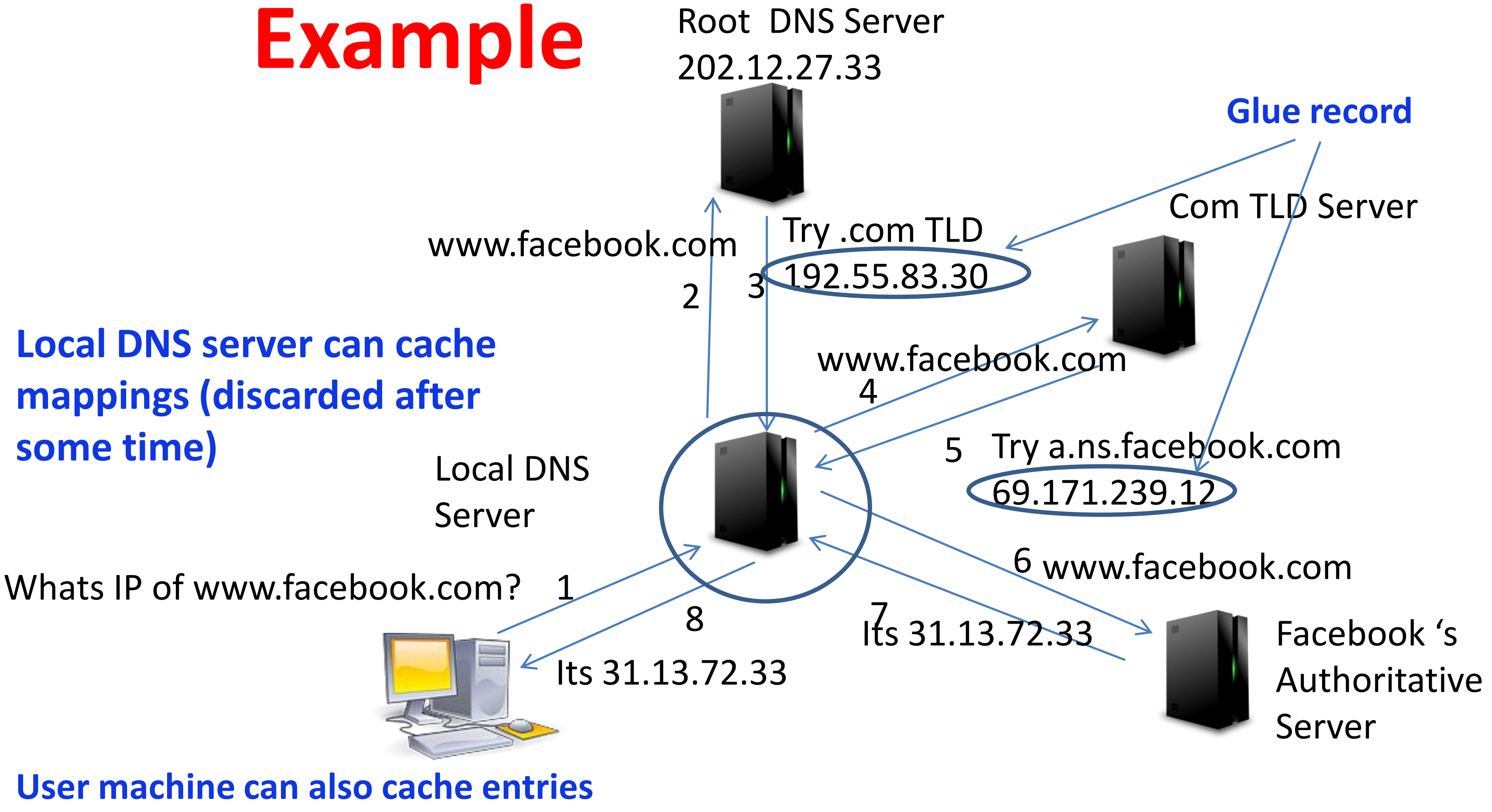
Top Level Domain Servers
E.g. Verisign company maintains TLD servers for “com” domain



Authoritative DNS Servers:
Each organization maintains its own DNS servers

Local DNS Server:
Provides DNS service to hosts within an organization
Hosts obtain local DNS server’s IP address often via DHCP

Example



Root DNS Server
202.12.27.33
Glue record
Com TLD Server
www.facebook.com
2
3
Try .com TLD
192.55.83.30
Local DNS server can cache mappings (discarded after some time)
www.facebook.com
4
5
Try a.ns.facebook.com
69.171.239.12
Local DNS
Server
6 www.facebook.com
Whats IP of www.facebook.com?
1
8
7
Its 31.13.72.33
Its 31.13.72.33
Facebook 's
Authoritative
Server
User machine can also cache entries

DNS Server Database

- Store Resource Records (RRs)
- Four Tuple: [Name, Value, Type, TTL]
- Type=A; Name: Hostname; Value: IP Address
  - E.g. [star.c10r.facebook.com, 31.13.72.33, A, 17]
- Type=NS; Name: Domain; Value: host-name of the authoritative name server
  - E.g. [facebook.com, a.ns.facebook.com, NS, 172797]

DNS Database

- Type=CNAME; Name: Hostname; Value: Canonical hostname
  – E.g. [www.facebook.com, star.c10r.facebook.com, CNAME, 2362]
- Type=MX; Name: Hostname; Value: Canonical name of the mail server
  – E.g. [facebook.com, msgin.t.facebook.com, MX, 300]

Rules

- An authoritative name server (for a given host) will always contain type A record of that host
- A non-authoritative name server will contain a type NS record for the domain and the type A record of the domain's authoritative server
  - [facebook.com, a.ns.facebook.com, NS, 172797]
  - [a.ns.facebook.com, 69.171.239.12, A, 172575]
- Demo: Dig command

DNS Message Format

Query/reply; Authoritative flag;
Recursion desired;
Recursion available

0 31

Identification	Flags
Number of questions	Number of answer RRs
Number of authority RRs	Number of additional RRs
Questions	
Answers	
Authority	
Additional Information	

DNS runs over UDP and uses port 53

DNS Vulnerabilities

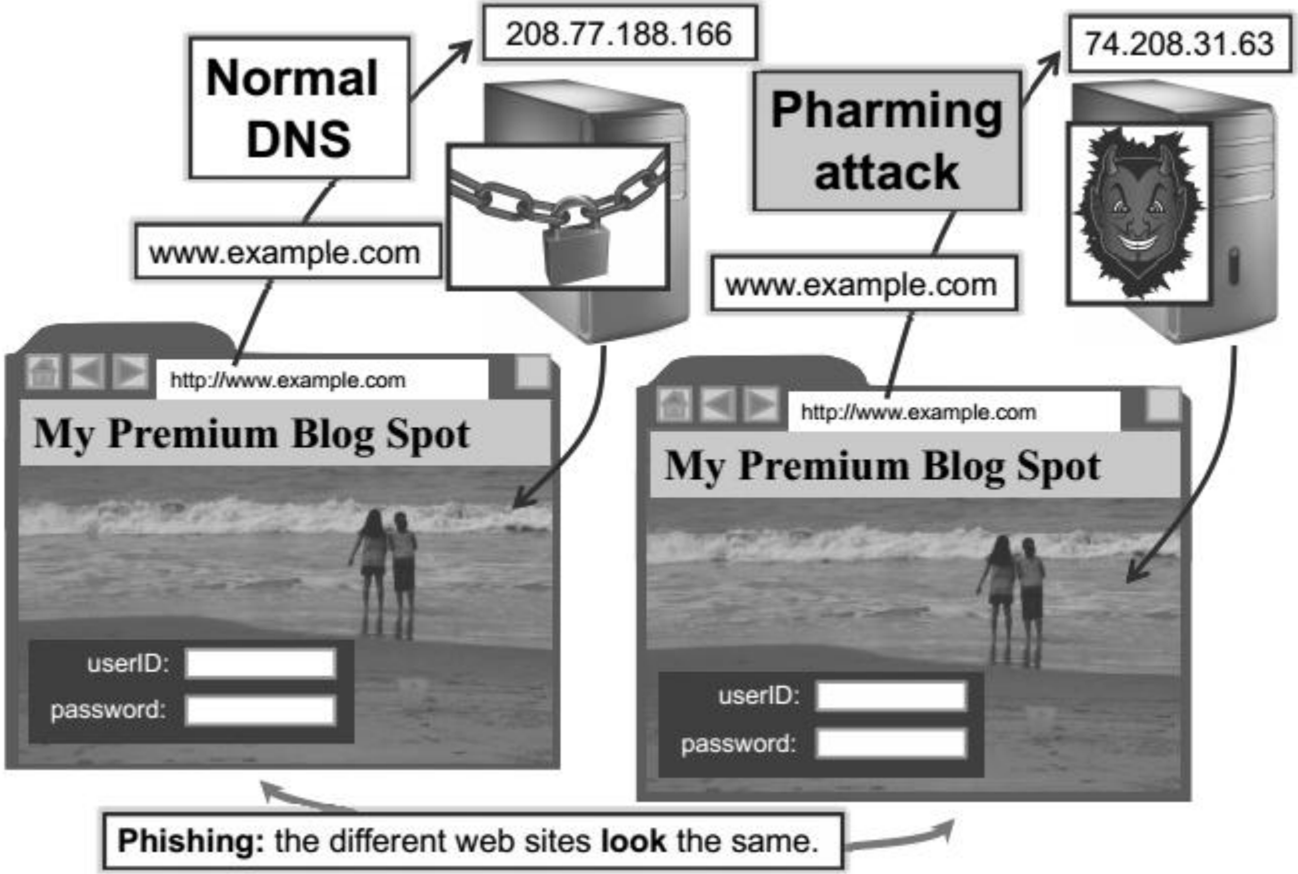
- No authentication of DNS responses
  - Relies solely on a 16-bit identification field
- Can insert fake records in cache via Glue records

Attacks: Pharming and Phising

- Pharming: Hostname resolves to false address (of malicious host)
  - Host can be web server, mail server, OS update server
  - Very dangerous; DNS core service in Internet
  - When cached in local DNS, many downstream clients affected
- Web server: Phising is where false website is near identical to original website
  - Malicious host can steal info, pass on malware
  - No easy way to detect

Attacks: Pharming and Phising

- Mail server pharming → can access mails
  - Passwords recovery of many sites often happens via emails
- OS update server pharming
  - Can pass on malicious code


Normal DNS
208.77.188.166
www.example.com
http://www.example.com
My Premium Blog Spot
userID:
password:
Pharming attack
74.208.31.63
www.example.com
http://www.example.com
My Premium Blog Spot
userID:
password:
Phishing: the different web sites **look** the same.

How is Pharming done?

Many ways….

- **Rogue DNS server:** Suppose DNS server of iitd turned rogue. How can it poison cache and capture web traffic of say iitb ?

```
;QUESTION
www.iitd.ac.in. IN A
;ANSWER
www.iitd.ac.in. 8600 IN A 103.27.9.20
;AUTHORITY
iitd.ac.in. 8600 IN NS dns10.iitd.ac.in.
iitd.ac.in. 8600 IN NS dns8.iitd.ac.in.
;ADDITIONAL
dns8.iitd.ac.in. 8600 IN A 103.27.8.1
dns10.iitd.ac.in. 8600 IN A 103.27.10.1
```

- Suppose a user (anywhere) contacts its local DNS to resolve www.iitd.ac.in
- Local DNS contacts DNS server of iitd (rogue)
- Reply from rogue DNS →
- 105.2.10.5 is a malicious web server (phising)
- Local DNS caches www.iitb.ac.in to 105.2.10.5 (attacker's web site) for 8600 sec (can be set longer also)
- All clients of 'local DNS' when they want to reach www.iitb.ac.in, land up on attacker's site

```
;QUESTION
www.iitd.ac.in. IN A
;ANSWER
www.iitd.ac.in. 8600 IN A 103.27.9.20
;AUTHORITY
iitd.ac.in. 8600 IN NS dns10.iitd.ac.in.
iitd.ac.in. 8600 IN NS www.iitb.ac.in
;ADDITIONAL
www.iitb.ac.in. 8600 IN 105.2.10.5
dns10.iitd.ac.in. 8600 IN A 103.27.10.1
```

- Solution: Don't accept additional records unless the belong to the same domain

;QUESTION

www.iitd.ac.in. IN A

;ANSWER

www.iitd.ac.in. 8600 IN A 103.27.9.20

;AUTHORITY

iitd.ac.in. 8600 IN NS dns10.iitd.ac.in.

iitd.ac.in. 8600 IN NS www.iitb.ac.in.

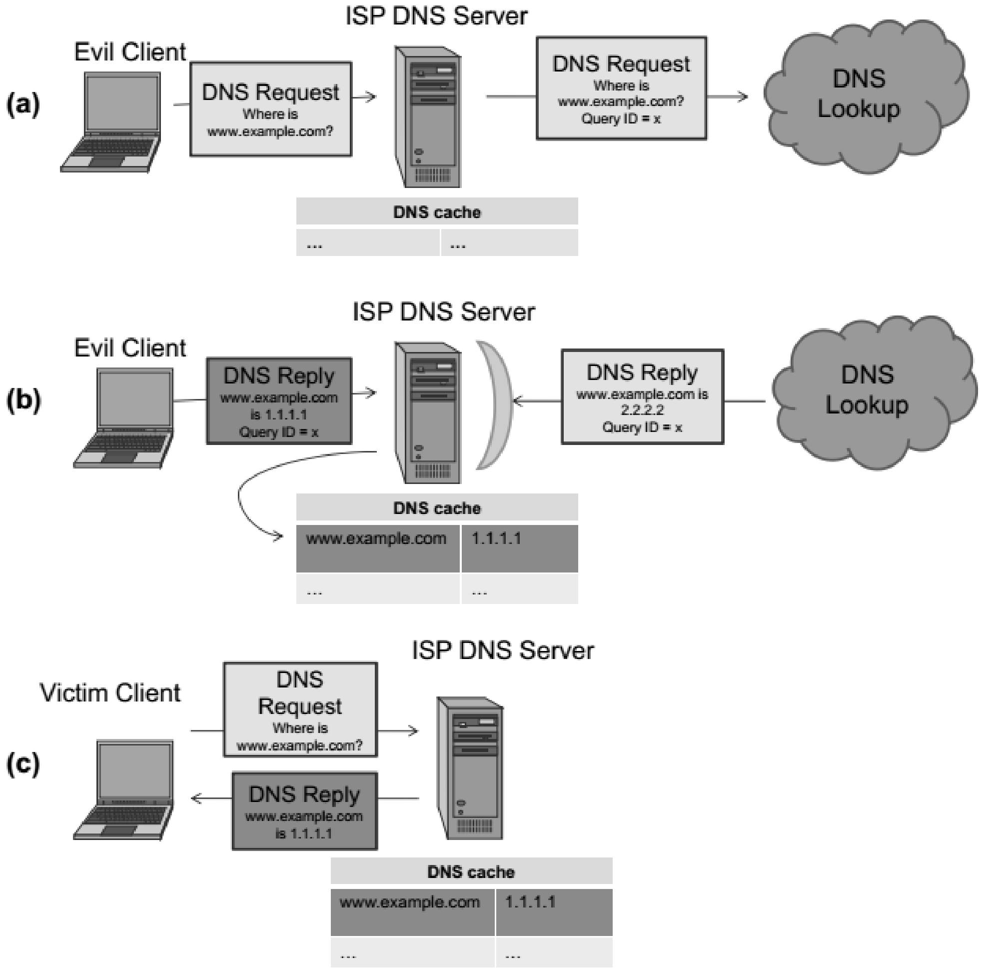
;ADDITIONAL

~~www.iitb.ac.in. 8600 IN A 105.2.10.5~~

dns10.iitd.ac.in. 8600 IN A 103.27.10.1

On-Path DNS Attack

- Attacker wants to poison cache of an ISP's DNS server
- Attacker can sniff packets (DNS requests) sent by ISP's DNS server
- Attack Details: Can easily spoof a DNS reply
  - Sniffing requests (request id, Src/dest IP/port) helps construct appropriate reply
  - Attacker can trigger specific requests by querying the ISP's DNS server for the same
  - Attack succeeds only if spoofed DNS reply reaches ISP's DNS server faster than one from authoritative server

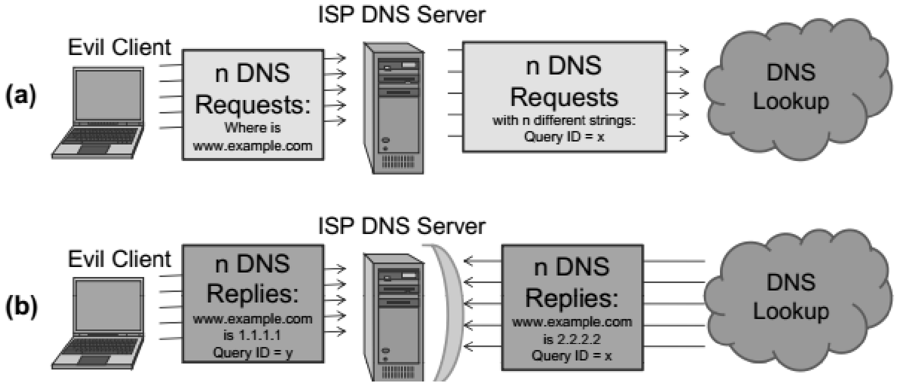


(a)
Evil Client
DNS Request
Where is www.example.com?
ISP DNS Server
DNS Request
Where is www.example.com?
Query ID = x
DNS Lookup
DNS cache
...
...
(b)
Evil Client
DNS Reply
www.example.com is 1.1.1.1
Query ID = x
ISP DNS Server
DNS Reply
www.example.com is 2.2.2.2
Query ID = x
DNS Lookup
DNS cache
www.example.com
1.1.1.1
...
...
(c)
Victim Client
DNS Request
Where is www.example.com?
DNS Reply
www.example.com is 1.1.1.1
ISP DNS Server
DNS cache
www.example.com
1.1.1.1
...
...

Off-Path (Blind) DNS Attack

- Guessing id tough (src/dst port often 53; IP addresses easy to figure out)
- Earlier DNS servers incremented id by 1 for every request
- Attack Details:
  - Send two DNS queries back to back (say www.evil.com and www.iitb.ac.in) to ISP's DNS server
  - First query will come to attacker's authoritative DNS for resolution , determine id x used
  - Spoof a reply to second query with id x+1
  - ISP's cache entry for www.iitb.ac.in poisoned (if spoofed reply faster)

- Solution: Use random id
- Birthday Paradox: Send large number of requests and fake replies
  - For N=213 (requests as well as fake replies), 50% chance one of the fake matches one of the requests
  - Challenge: race against time to beat replies from authoritative server
  - Authentic reply once cached, can be long wait before next attack



Sub-domain DNS Attack

- Any way to avoid race against time?
- Issue many requests (N) for non-existent sub-domains (e.g. aaa.example.com, aab.example.com etc)
- Authoritative name server ignores such requests → no race against time
- But only non-existent sub-domain poisoned. How does it help?

- Include a glue record
  - Name server of example.com maps to attacker's IP
  - Can alter name resolutions for the entire domain

Defences

- Most DNS attacks target local DNS servers → local DNS servers should accept only internal requests
- Source port randomization: Apart from ID randomize the src port from which requests are made
  - Space: 2^16 possible ids times ~64000 possible ports

DNSSEC

- Solutions are only stop gap measures, better approach secure DNS → DNSSEC
- All DNS replies digitally signed
  - Based on chain of trust model
  - .com vouches for example.com; example.com vouches for another.example.com
- Requires changes to both client and server
- An ongoing deployment effort