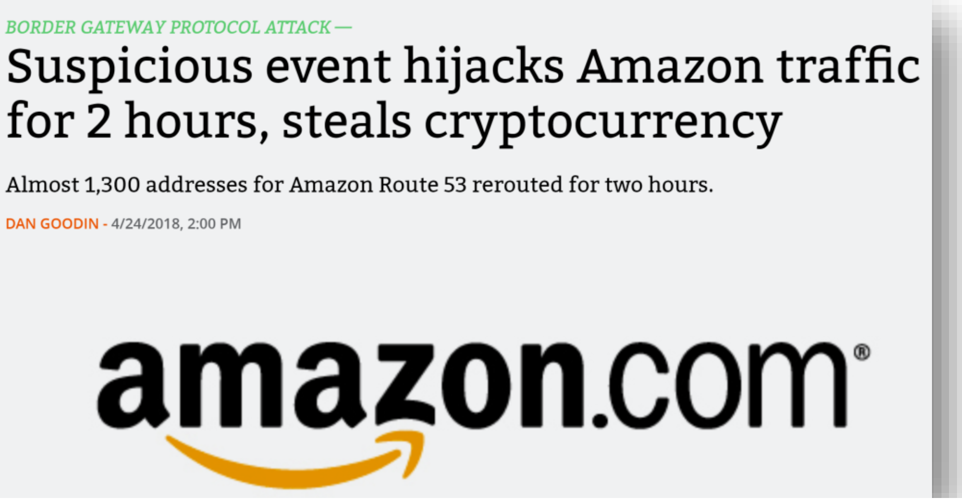
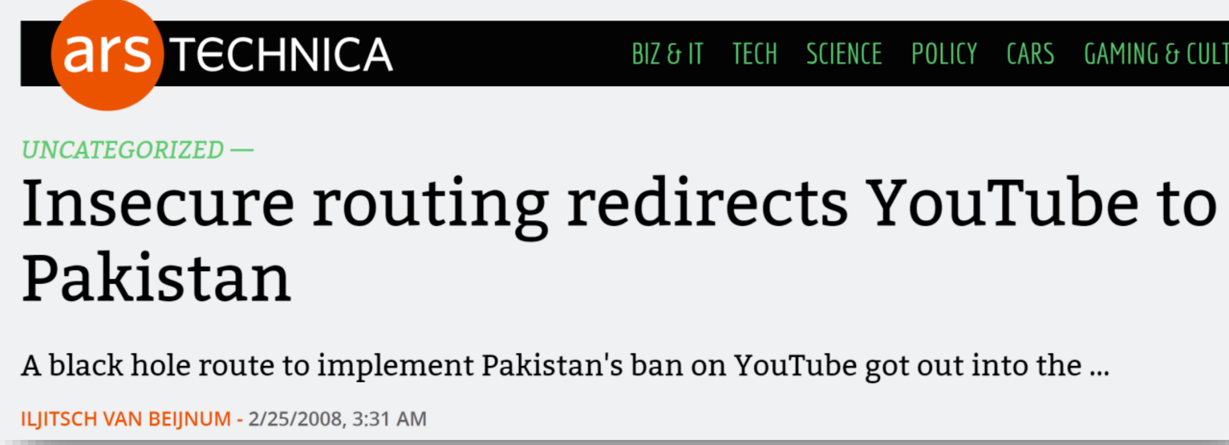


BORDER GATEWAY PROTOCOL ATTACK —

Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency

Almost 1,300 addresses for Amazon Route 53 rerouted for two hours.

DAN GOODIN - 4/24/2018, 2:00 PM



UNCATEGORIZED —

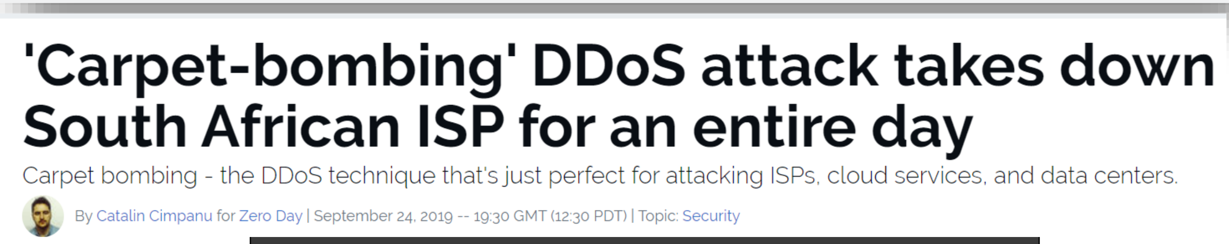
Insecure routing redirects YouTube to Pakistan

A black hole route to implement Pakistan's ban on YouTube got out into the ...

ILJITSCH VAN BEIJNUM - 2/25/2008, 3:31 AM

University Security

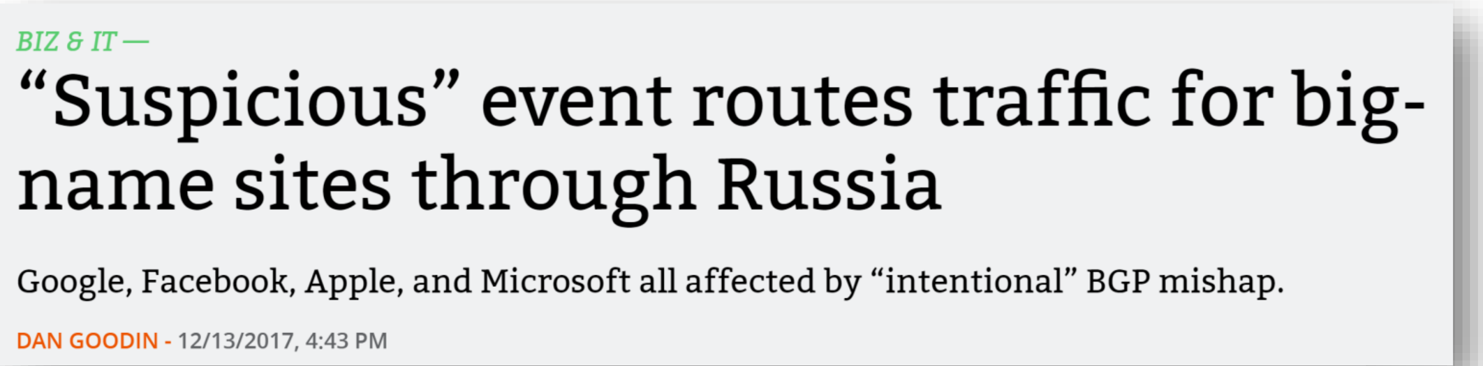
86% of Education Industry Experienced DNS Attack in Past Year



'Carpet-bombing' DDoS attack takes down South African ISP for an entire day

Carpet bombing - the DDoS technique that's just perfect for attacking ISPs, cloud services, and data centers.

By Catalin Cimpanu for Zero Day | September 24, 2019 -- 19:30 GMT (12:30 PDT) | Topic: Security

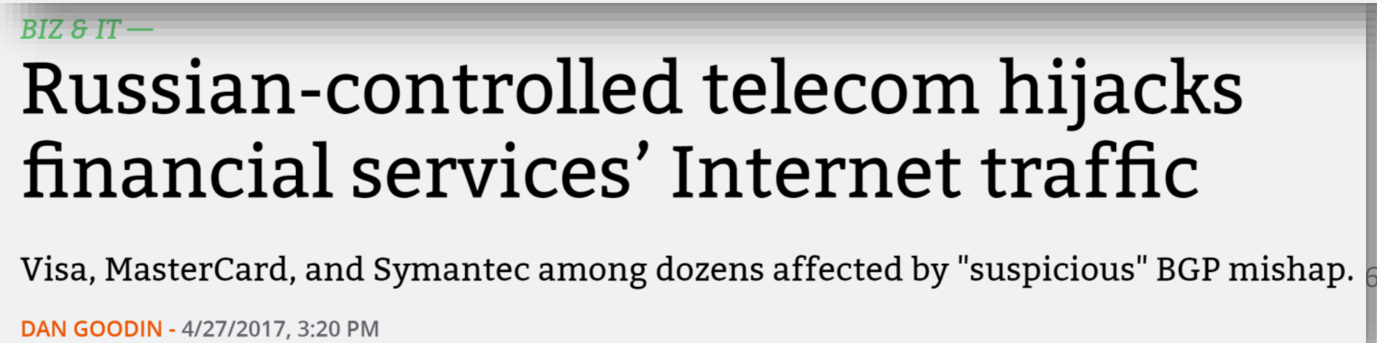


BIZ & IT —

“Suspicious” event routes traffic for big-name sites through Russia

Google, Facebook, Apple, and Microsoft all affected by “intentional” BGP mishap.

DAN GOODIN - 12/13/2017, 4:43 PM



BIZ & IT —

Russian-controlled telecom hijacks financial services’ Internet traffic

Visa, MasterCard, and Symantec among dozens affected by "suspicious" BGP mishap.

DAN GOODIN - 4/27/2017, 3:20 PM

Network Security

CS 642

UW Madison

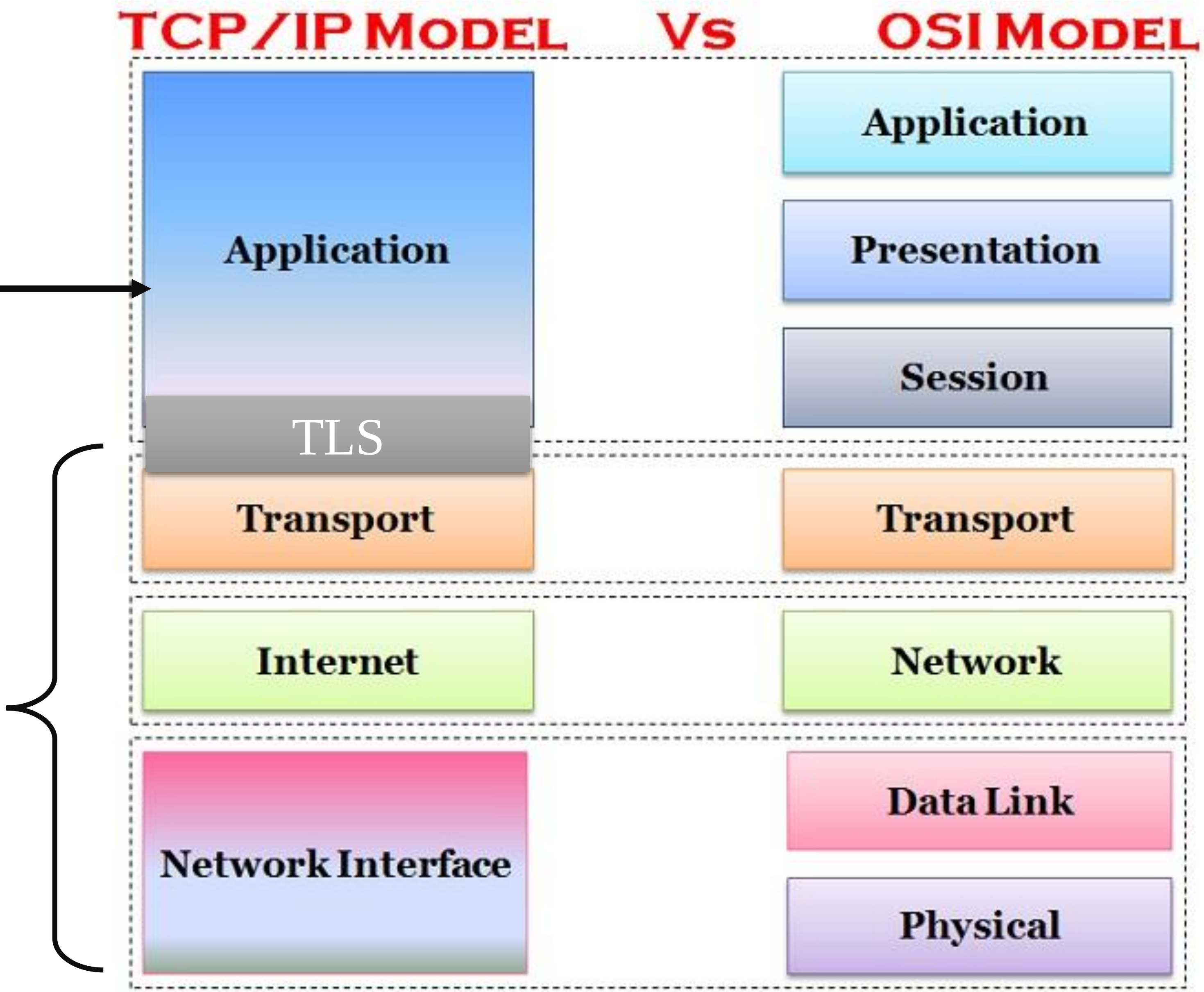
Earlence Fernandes

DNS and BGP

Oct 8, 2019

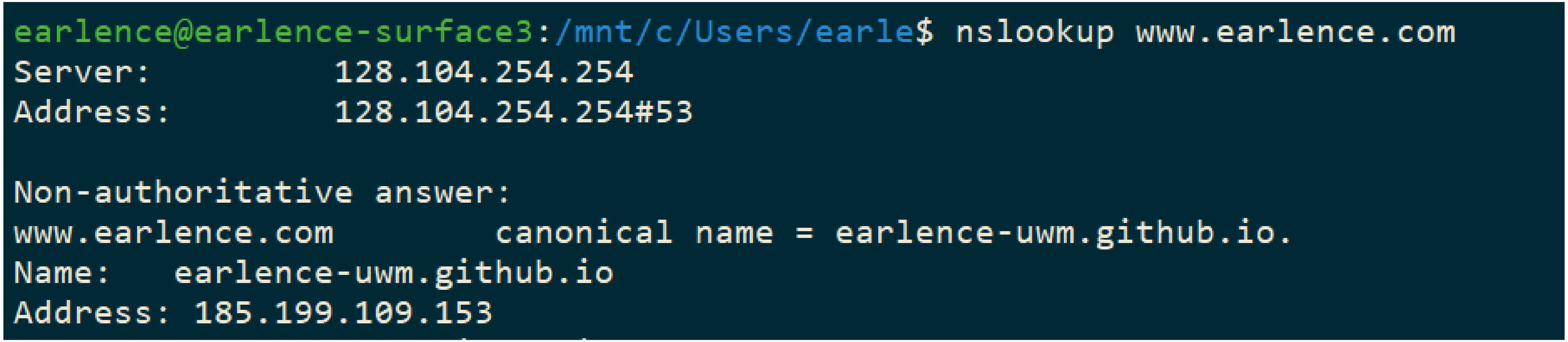
Web Security

Network Security



128.105.37.141

We don’t want to have to remember IP addresses



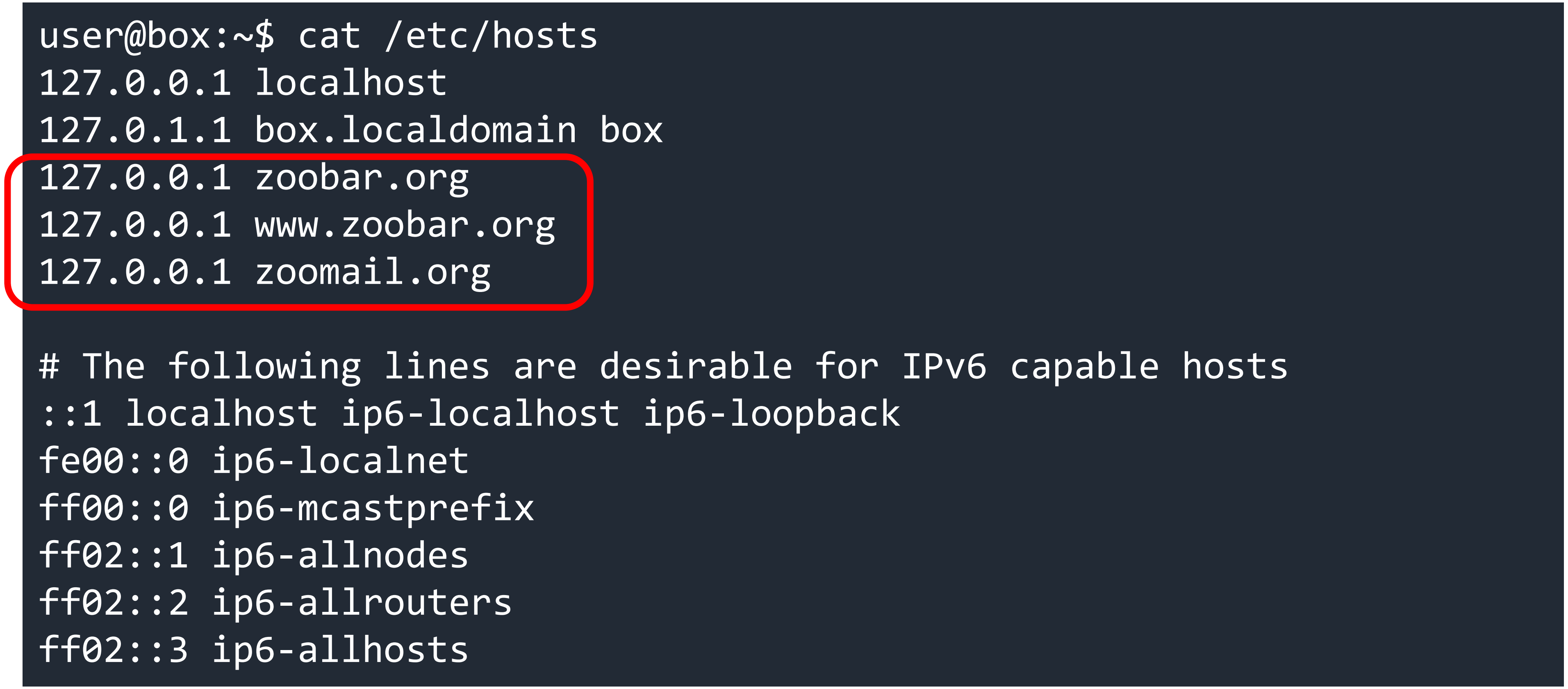
```
earlence@earlence-surface3:/mnt/c/Users/earle$ nslookup www.earlence.com
Server:         128.104.254.254
Address:        128.104.254.254#53

Non-authoritative answer:
www.earlence.com        canonical name = earlence-uwm.github.io.
Name:   earlence-uwm.github.io
Address: 185.199.109.153
```

Early days of ARPANET:
manually managed `hosts.txt`
served from single computer at SRI

128.105.37.141

We don’t want to have to remember IP addresses



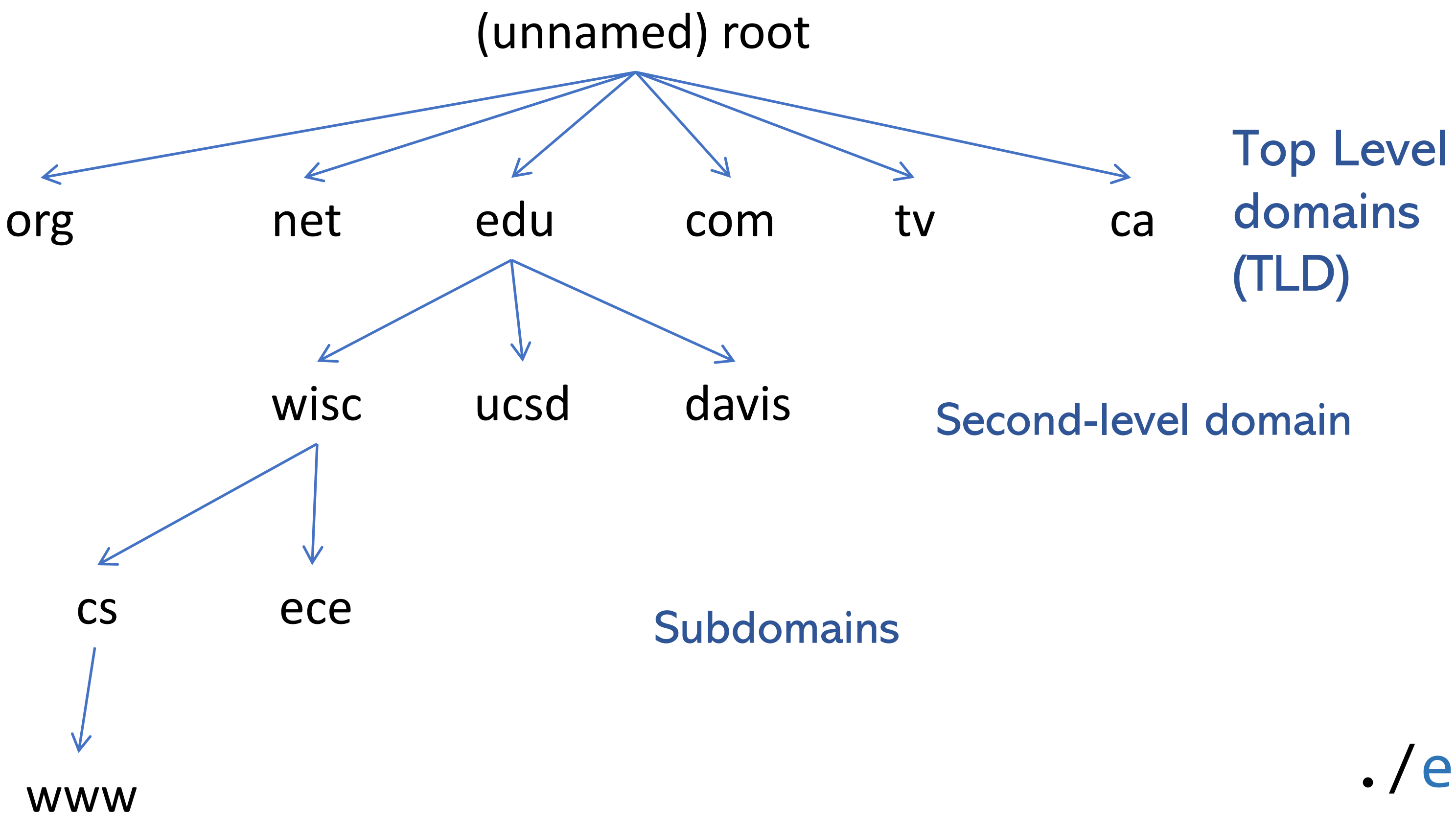
```
user@box:~$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 box.localdomain box
127.0.0.1 zoobar.org
127.0.0.1 www.zoobar.org
127.0.0.1 zoomail.org

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

Early days of ARPANET: manually managed

`hosts.txt` served from single computer at SRI

Hierarchical domain namespace



(unnamed) root

org net edu com tv ca

wisc ucsd davis

cs ece

www

Top Level domains (TLD)

Second-level domain

Subdomains

Separated by '.'

FQDN: Fully qualified domain name

`seclab-1.cs.wisc.edu`

Hostname Subdomain Domain TLD

`./edu/wisc/cs/seclab-1`

max 63 characters

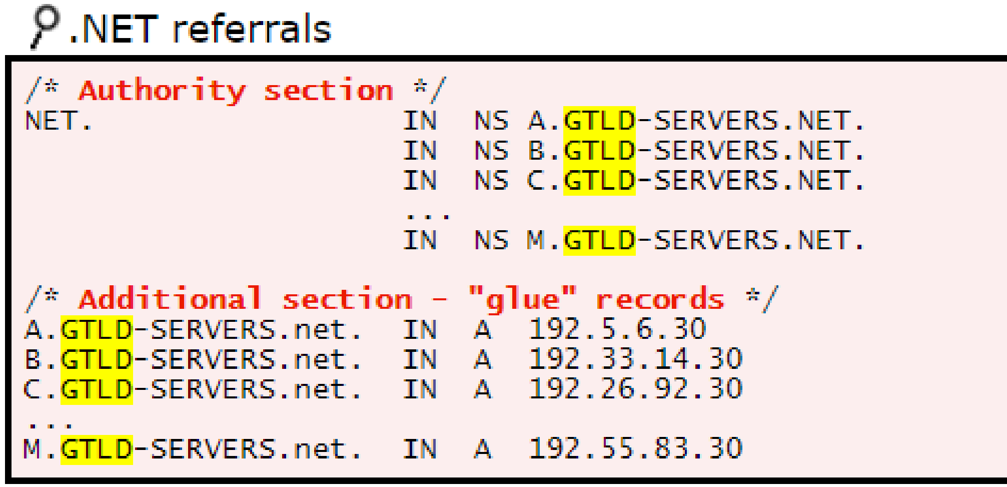
Internet-wide namespace

- ICANN (Internet Corporation for Assigned Names and Numbers)

- DNS Servers
  - DNS resolver
  - root nameservers – 13 of them worldwide **A** through **M**
  - authoritative nameservers – authorized to provide IP for a (sub)domain / hostname

- Zone: a contiguous portion of **domain namespace**
  - A subtree

```
A.ROOT-SERVERS.NET. IN A 198.41.0.4
B.ROOT-SERVERS.NET. IN A 192.228.79.201
C.ROOT-SERVERS.NET. IN A 192.33.4.12
...
M.ROOT-SERVERS.NET. IN A 202.12.27.33
```

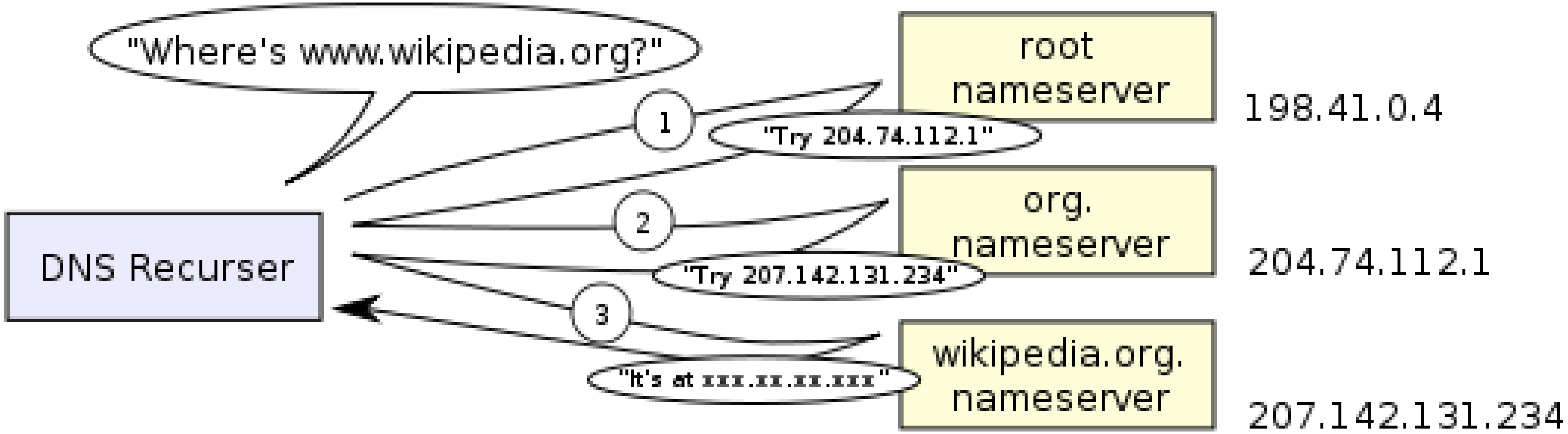


.NET referrals

```
/* Authority section */
NET.                 IN   NS A.GTLD-SERVERS.NET.
                     IN   NS B.GTLD-SERVERS.NET.
                     IN   NS C.GTLD-SERVERS.NET.
                     ...
                     IN   NS M.GTLD-SERVERS.NET.

/* Additional section - "glue" records */
A.GTLD-SERVERS.net.  IN   A   192.5.6.30
B.GTLD-SERVERS.net.  IN   A   192.33.14.30
C.GTLD-SERVERS.net.  IN   A   192.26.92.30
...
M.GTLD-SERVERS.net.  IN   A   192.55.83.30
```

Resolving names



From: http://en.wikipedia.org/wiki/File:An_example_of_theoretical_DNS_recursion.svg

Example DNS record (and query) types

A	Address mapping record (get me an IPv4 address)
AAAA	Same for IPv6 address
NS	name server, the DNS zone
TXT	machine readable text data, has been used for many things, including encryption mechanisms, policy
MX	mail exchange (SMTP mail server for the domain)
CNAME	Canonical name, alias of a domain

Caching

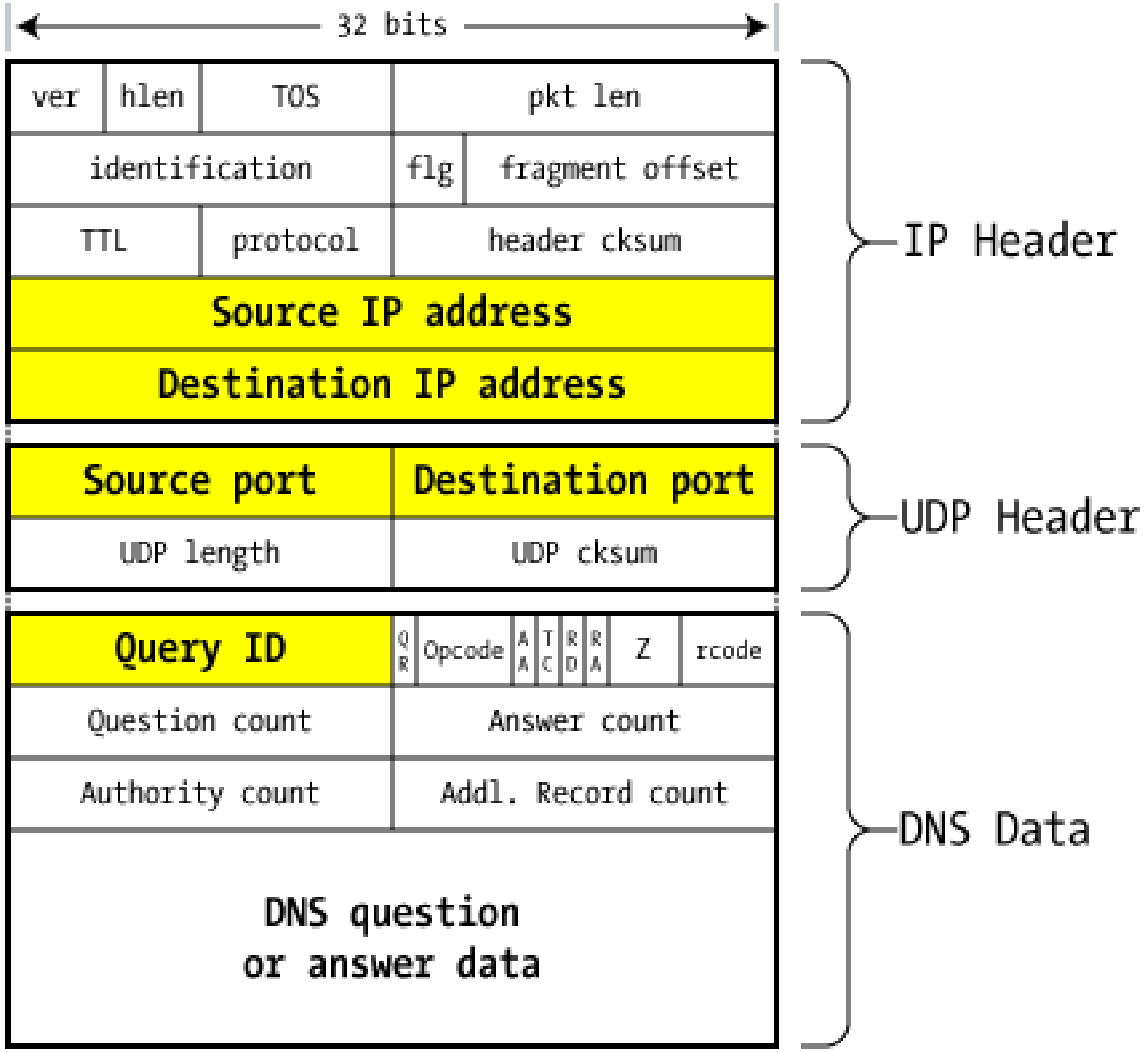
- DNS servers will cache responses
  - Both negative and positive responses
  - Speeds up queries
  - periodically times out. TTL set by data owner

DNS packet on wire

We'll walk through the example from Friedl's document (on Canvas)

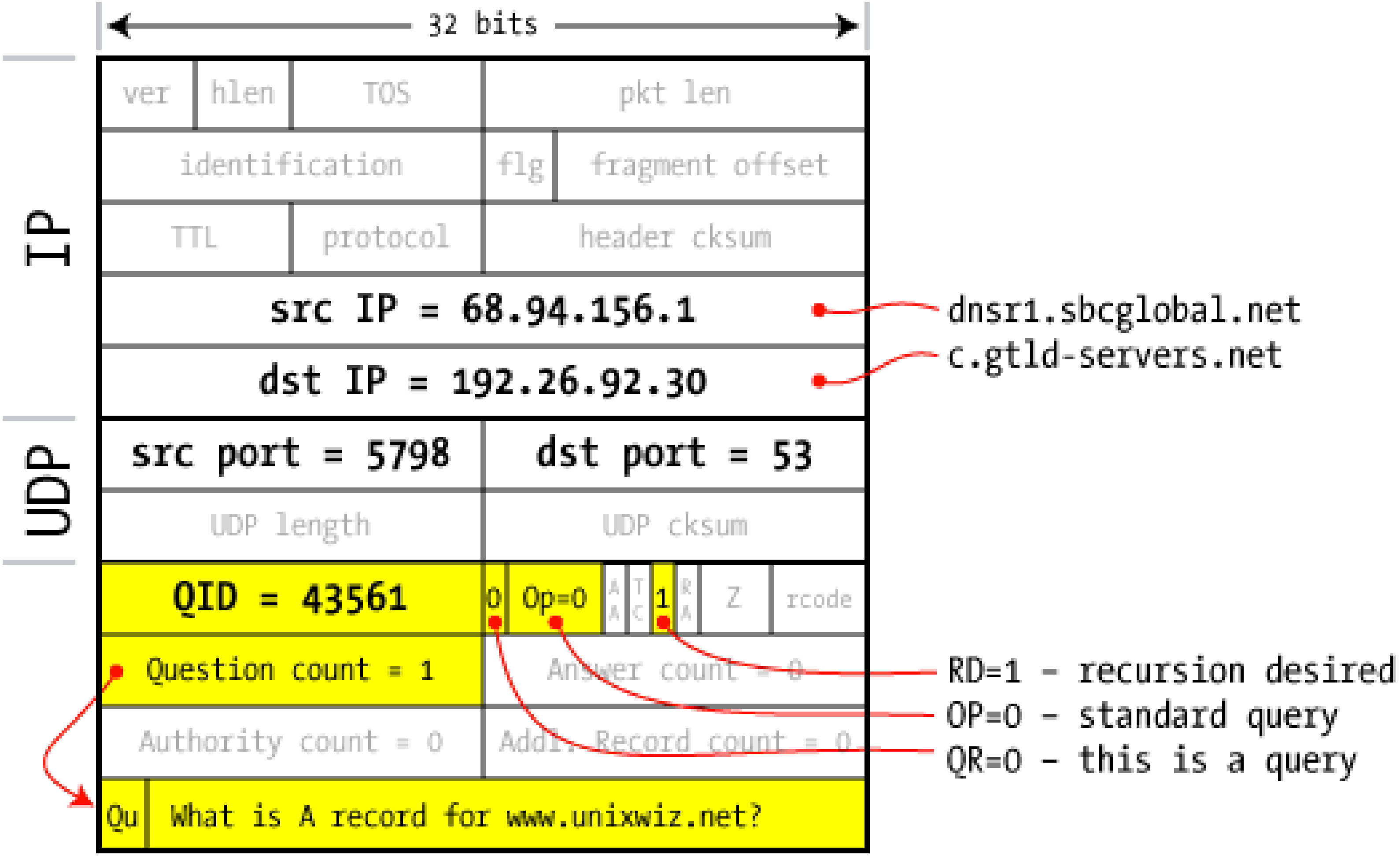
`www.unixwiz.net`

Query ID is 16-bit value



From Friedl explanation of DNS cache poisoning, as are following diagrams

Query from resolver to NS



32 bits

IP

ver | hlen | TOS | pkt len

identification | flg | fragment offset

TTL | protocol | header cksum

src IP = 68.94.156.1

dst IP = 192.26.92.30

UDP

src port = 5798 | dst port = 53

UDP length | UDP cksum

QID = 43561 | 0 | Op=0 | AA | TC | 1 | RA | Z | rcode

Question count = 1 | Answer count = 0

Authority count = 0 | Addl Record count = 0

Qu | What is A record for www.unixwiz.net?

dnsr1.sbcglobal.net

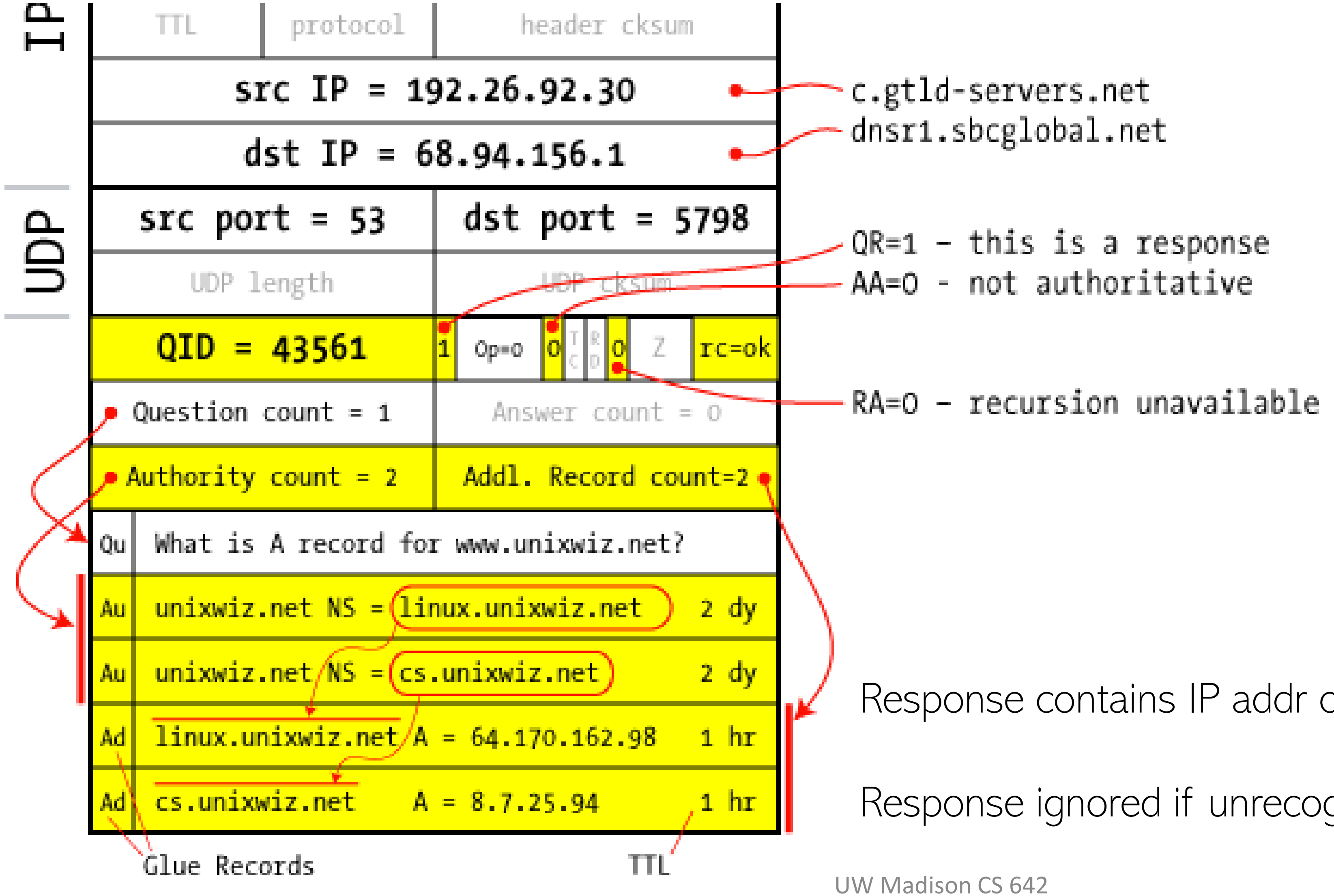
c.gtld-servers.net

RD=1 - recursion desired

OP=0 - standard query

QR=0 - this is a query

Reply from NS to Resolver



src IP = 192.26.92.30

dst IP = 68.94.156.1

src port = 53

dst port = 5798

QID = 43561

rc=ok

Question count = 1

Answer count = 0

Authority count = 2

Addl. Record count=2

Qu What is A record for www.unixwiz.net?

Au unixwiz.net NS = linux.unixwiz.net 2 dy

Au unixwiz.net NS = cs.unixwiz.net 2 dy

Ad linux.unixwiz.net A = 64.170.162.98 1 hr

Ad cs.unixwiz.net A = 8.7.25.94 1 hr

c.gtld-servers.net

dnsr1.sbcglobal.net

QR=1 - this is a response

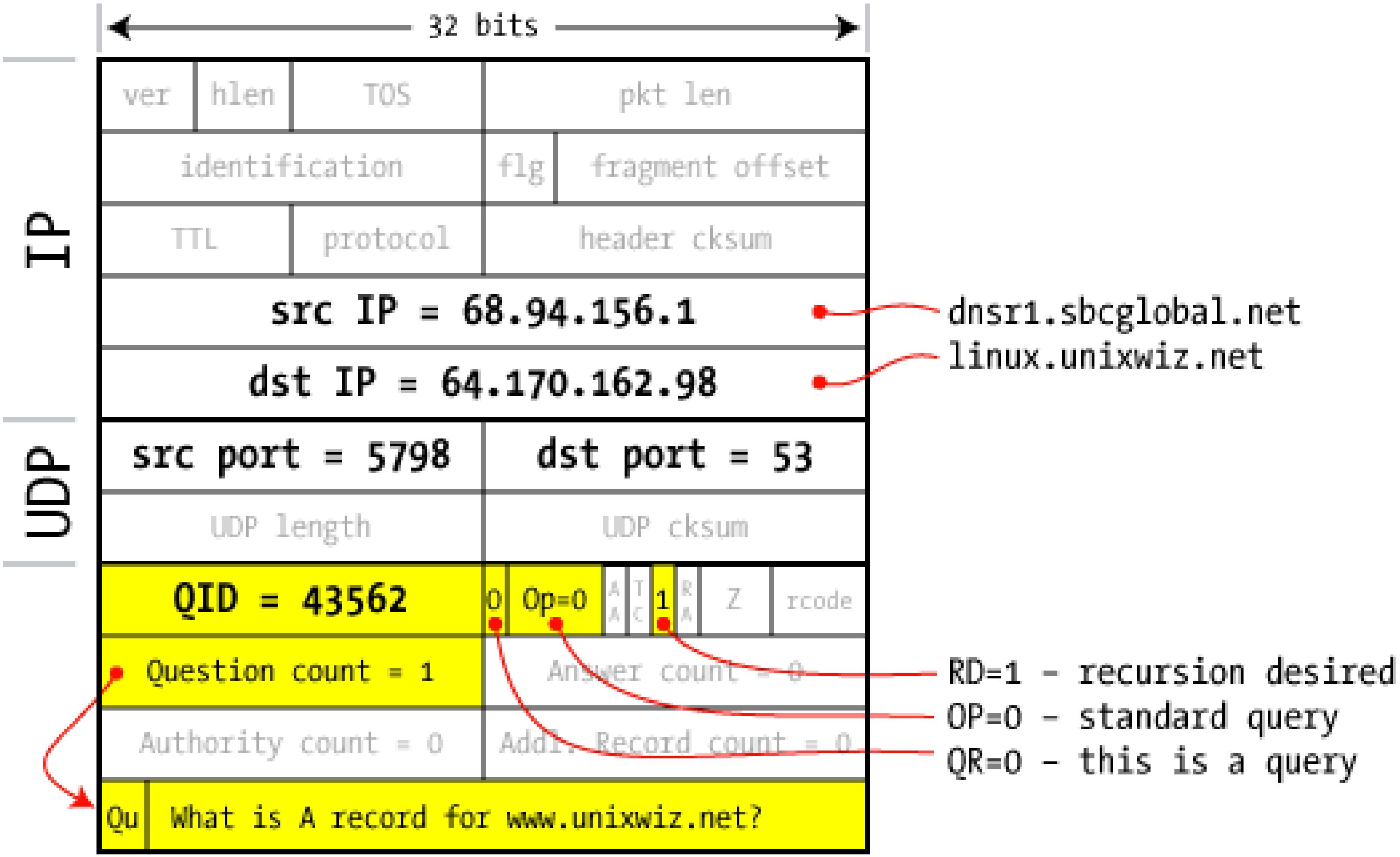
AA=0 - not authoritative

RA=0 - recursion unavailable

Response contains IP addr of next NS server (called "glue")

Response ignored if unrecognized QueryID

Query to Second NS



32 bits

IP

UDP

ver | hlen | TOS | pkt len

identification | flg | fragment offset

TTL | protocol | header cksum

src IP = 68.94.156.1

dst IP = 64.170.162.98

src port = 5798 | dst port = 53

UDP length | UDP cksum

QID = 43562 | 0 | Op=0 | AA | TC | 1 | RA | Z | rcode

Question count = 1 | Answer count = 0

Authority count = 0 | Addl. Record count = 0

Qu | What is A record for www.unixwiz.net?

dnsr1.sbcglobal.net

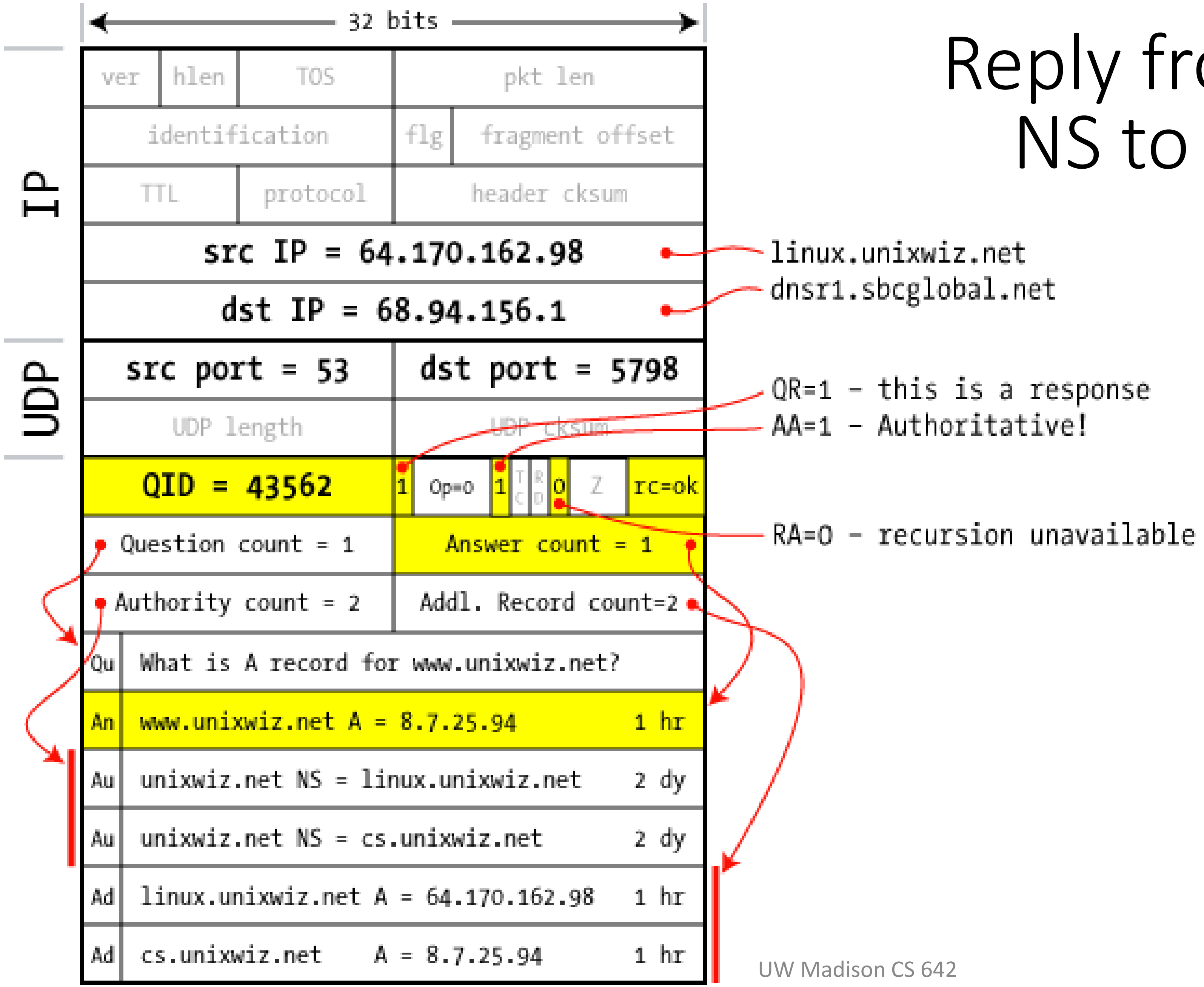
linux.unixwiz.net

RD=1 - recursion desired

OP=0 - standard query

QR=0 - this is a query

Reply from Second NS to Resolver



32 bits

IP

ver | hlen | TOS | pkt len

identification | flg | fragment offset

TTL | protocol | header cksum

src IP = 64.170.162.98 — linux.unixwiz.net

dst IP = 68.94.156.1 — dnsr1.sbcglobal.net

UDP

src port = 53 | dst port = 5798

UDP length | UDP cksum

QID = 43562 | 1 | Op=0 | 1 | TC | RD | 0 | Z | rc=ok

QR=1 - this is a response

AA=1 - Authoritative!

RA=0 - recursion unavailable

Question count = 1 | Answer count = 1

Authority count = 2 | Addl. Record count=2

Qu What is A record for www.unixwiz.net?

An www.unixwiz.net A = 8.7.25.94 1 hr

Au unixwiz.net NS = linux.unixwiz.net 2 dy

Au unixwiz.net NS = cs.unixwiz.net 2 dy

Ad linux.unixwiz.net A = 64.170.162.98 1 hr

Ad cs.unixwiz.net A = 8.7.25.94 1 hr

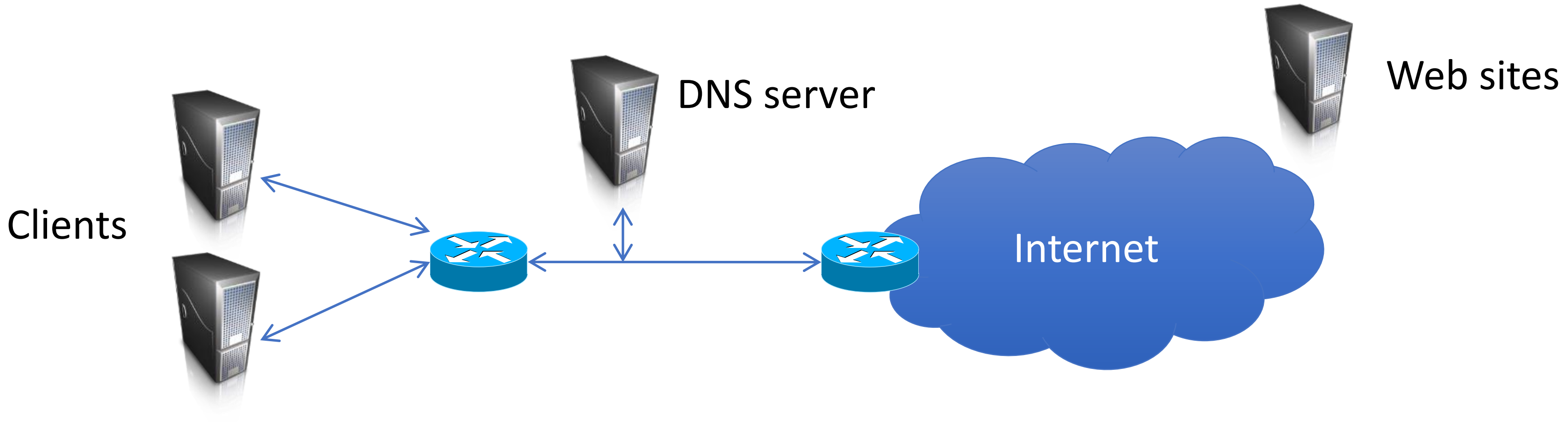
Caching is the key

- DNS servers are queried trillions of times, though they seem fast, doing it again and again could
  - burden the network
  - slowdown everything

- Therefore, authoritative responses are cached for limited amount of time
  - Both **NS** and **A** records are cached
  - TTL – how long to keep the DNS record in cache

- bailiwick checking response is cached if it is within the same domain of query
  - i.e. `ns.a.com` cannot set NS for `b.com`

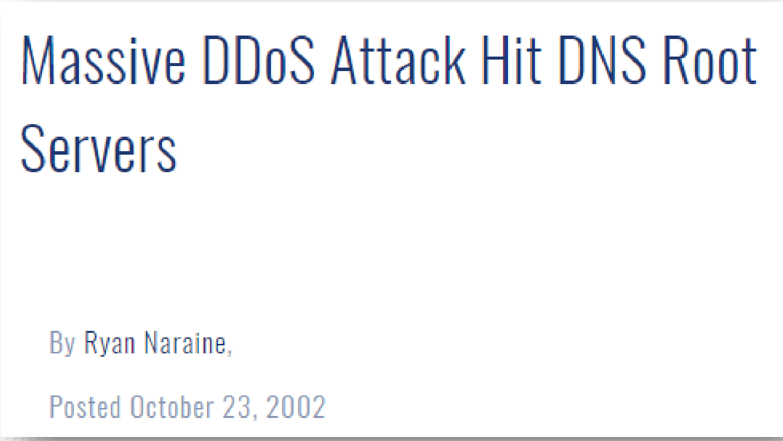
Attacks against DNS?



- Corrupted nameservers
- Intercept & manipulate requests
- DDoS
- Cache poisoning
- Phishing / typo squatting / piggy-backing

DDoS against DNS

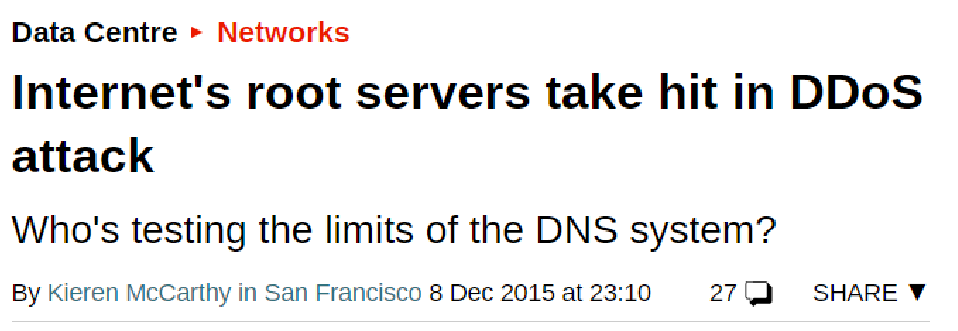
- Denial of Service
  - take down DNS server, clients can’t use Internet
  - Attack against root servers:



Massive DDoS Attack Hit DNS Root Servers

By Ryan Naraine,

Posted October 23, 2002



Data Centre ▸ Networks

Internet's root servers take hit in DDoS attack

Who's testing the limits of the DNS system?

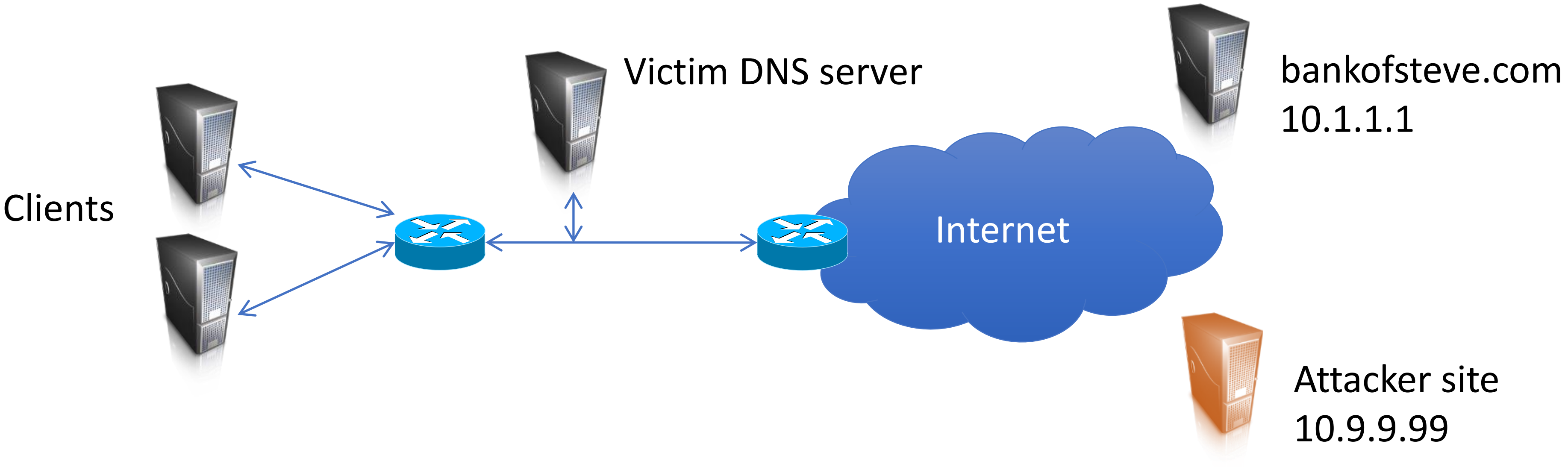
By Kieren McCarthy in San Francisco 8 Dec 2015 at 23:10 27 SHARE ▼

- DoD purportedly has interesting response:

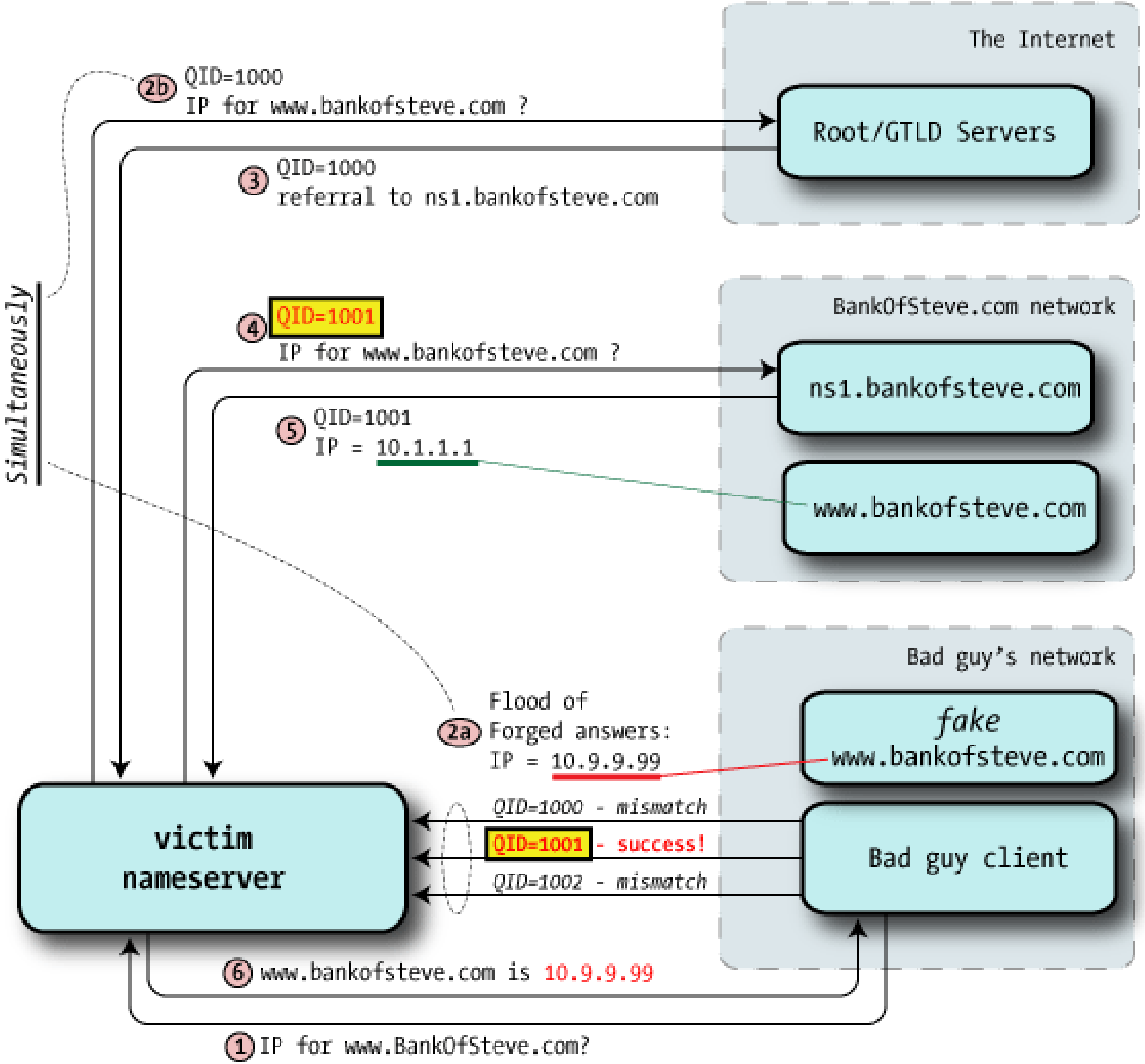
> *“In the event of a massive cyberattack against the country that was perceived as originating from a foreign source, the United States would consider launching a* ***counterattack or bombing the source of the cyberattack,*** *Hall said. But he noted the preferred route would be warning the source to shut down the attack before a military response.”*

http://www.computerworld.com/s/article/9010921/RSA_U.S._cyber_counterattack_Bomb_one_way_or_the_other

DNS cache poisoning

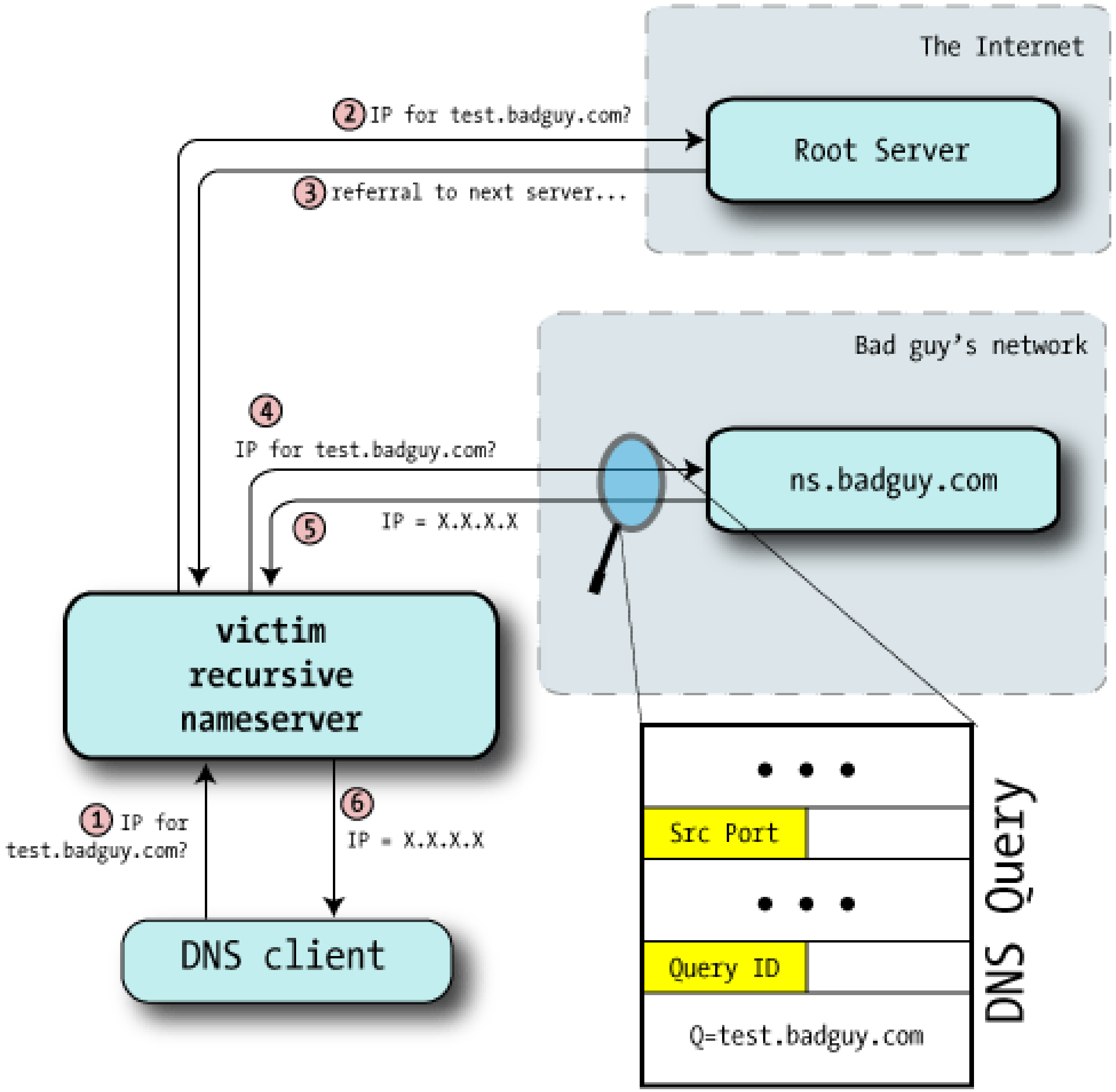


How might an attacker do this?
Assume DNS server uses predictable UDP port



The Internet
Root/GTLD Servers
2b QID=1000
IP for www.bankofsteve.com ?
3 QID=1000
referral to ns1.bankofsteve.com
Simultaneously
BankOfSteve.com network
ns1.bankofsteve.com
www.bankofsteve.com
4 QID=1001
IP for www.bankofsteve.com ?
5 QID=1001
IP = 10.1.1.1
Bad guy's network
fake
www.bankofsteve.com
Flood of
2a Forged answers:
IP = 10.9.9.99
QID=1000 - mismatch
QID=1001 - success!
QID=1002 - mismatch
victim
nameserver
Bad guy client
6 www.bankofsteve.com is 10.9.9.99
1 IP for www.BankOfSteve.com?

How to predict the query ID?

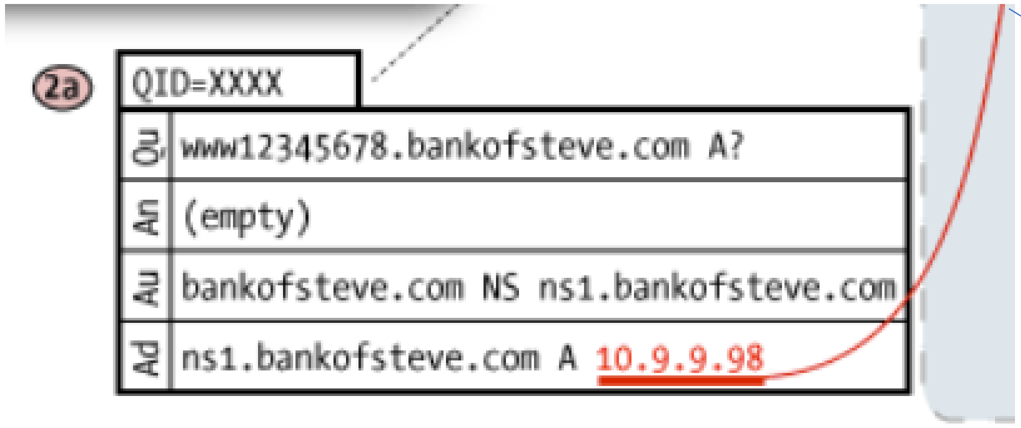


Another idea (Dan Kaminsky's attack):

- Poison cache for NS record instead
- Now can take over all of second level domain

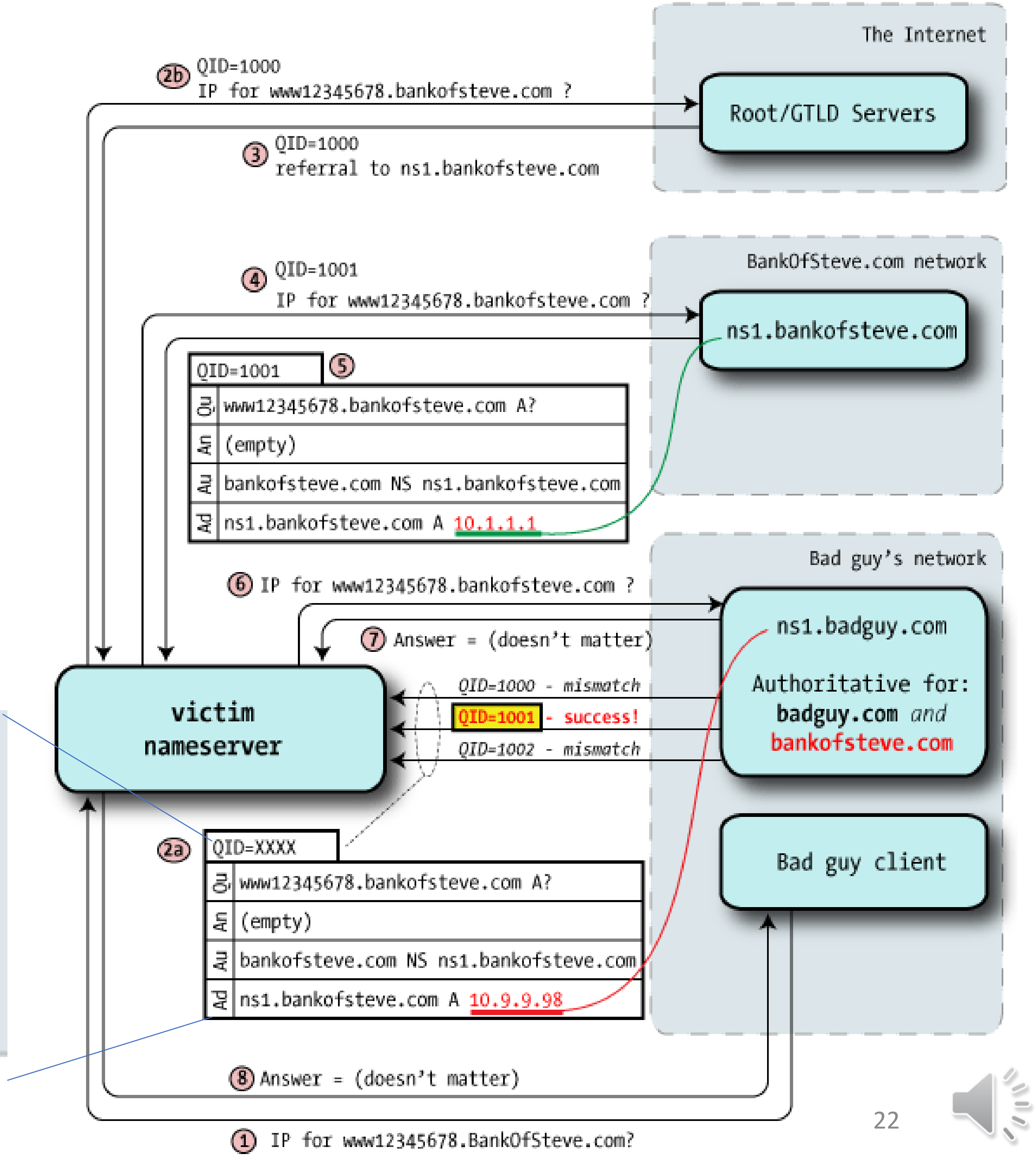
How many tries does this require?

- 16 bit query id field
- If choosing randomly: 256 (birthday)
- If predictable, choose in range



2a QID=XXXX

Qu	www12345678.bankofsteve.com A?
An	(empty)
Au	bankofsteve.com NS ns1.bankofsteve.com
Ad	ns1.bankofsteve.com A 10.9.9.98



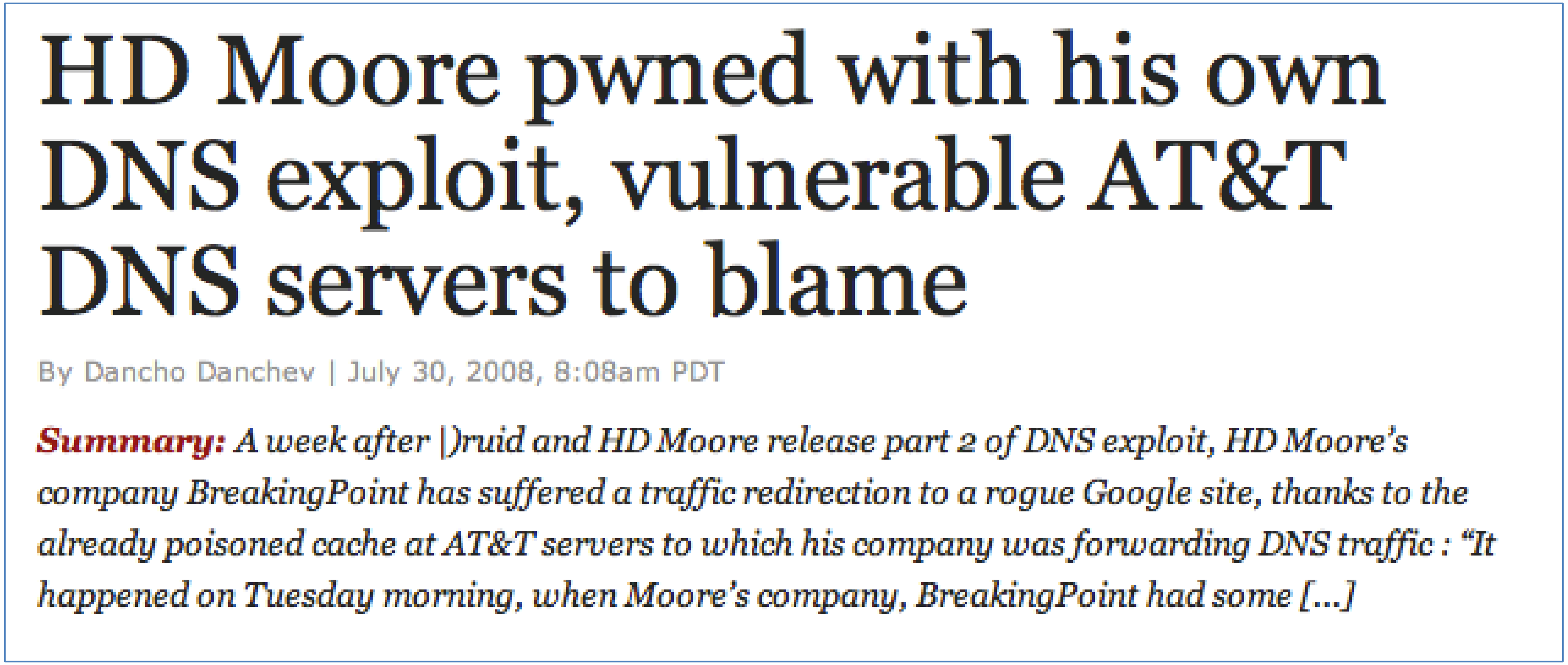
5 QID=1001

Qu	www12345678.bankofsteve.com A?
An	(empty)
Au	bankofsteve.com NS ns1.bankofsteve.com
Ad	ns1.bankofsteve.com A 10.1.1.1

2a QID=XXXX

Qu	www12345678.bankofsteve.com A?
An	(empty)
Au	bankofsteve.com NS ns1.bankofsteve.com
Ad	ns1.bankofsteve.com A 10.9.9.98

Does happen in the wild



HD Moore pwned with his own DNS exploit, vulnerable AT&T DNS servers to blame

By Dancho Danchev | July 30, 2008, 8:08am PDT

Summary: *A week after |)ruid and HD Moore release part 2 of DNS exploit, HD Moore's company BreakingPoint has suffered a traffic redirection to a rogue Google site, thanks to the already poisoned cache at AT&T servers to which his company was forwarding DNS traffic : "It happened on Tuesday morning, when Moore's company, BreakingPoint had some [...]*

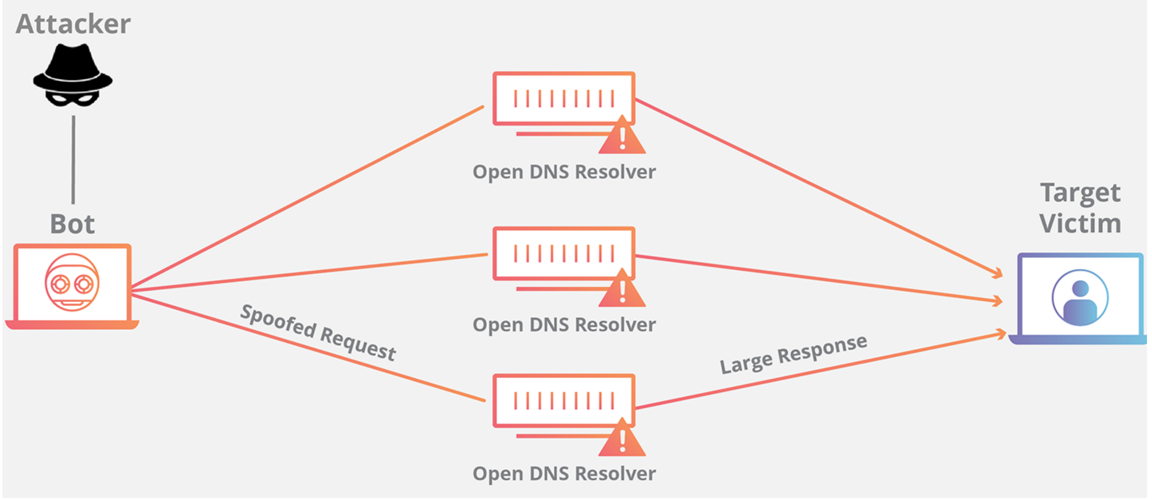
http://www.zdnet.com/blog/security/hd-moore-pwned-with-his-own-dns-exploit-vulnerable-at-t-dns-servers-to-blame/1608?tag=content;siu-container

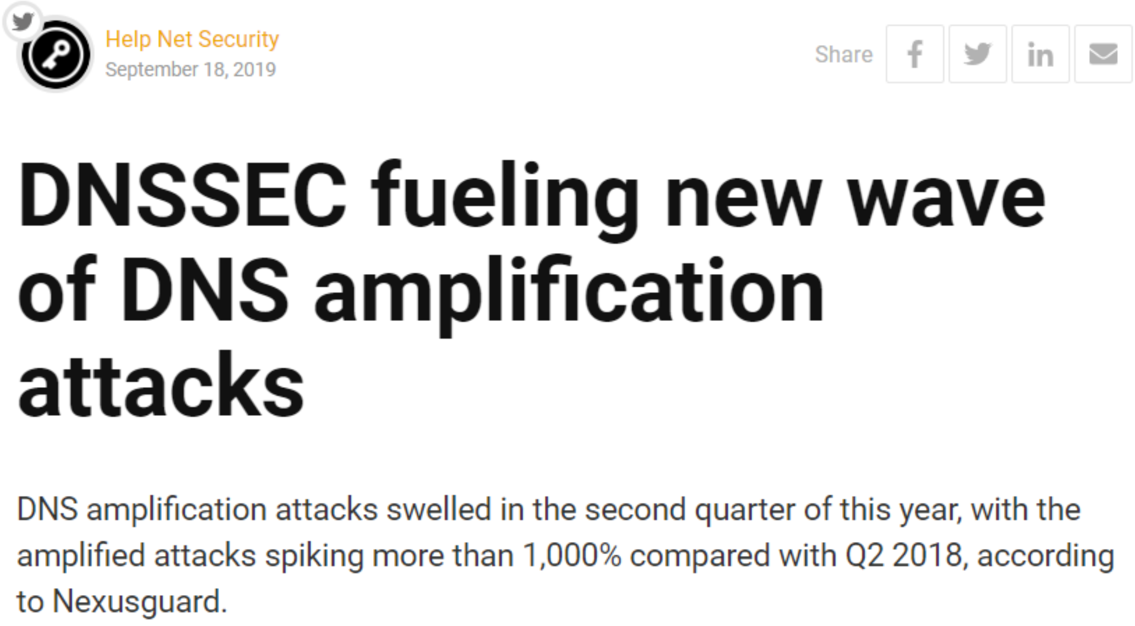
Defenses (and attacks)

- Query ID size is fixed at 16 bits
- Repeat each query with fresh Query ID
  - (randomize)
- Randomize UDP ports: not enough randomness in query ID only
- DNSsec
  - Cryptographically sign DNS responses, verify via chain of trust from roots on down

… but DNSSec vulnerable to DDoS

- Create large amount traffic from the DNS resolvers to the victim computer/server





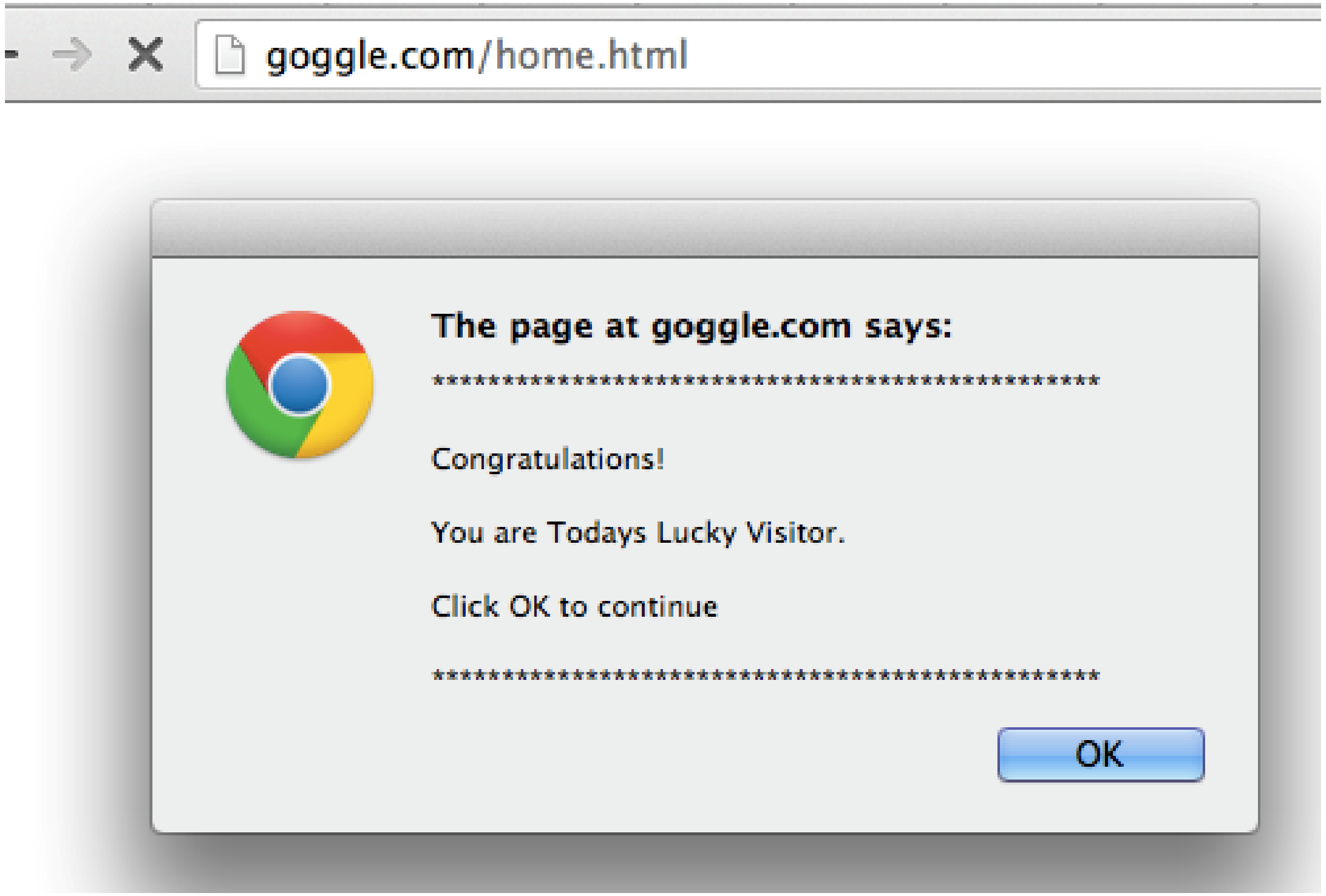
Help Net Security
September 18, 2019

DNSSEC fueling new wave of DNS amplification attacks

DNS amplification attacks swelled in the second quarter of this year, with the amplified attacks spiking more than 1,000% compared with Q2 2018, according to Nexusguard.

Phishing is common problem

- Typo squatting:
  - www.qpple.com
  - www.goggle.com
  - www.nytmes.com
- Other shenanigans:
  - www.badguy.com/(256 characters of filler)/www.google.com
- Phishing attacks
  - These just trick users into thinking a malicious domain name is the real one



goggle.com/home.html

The page at goggle.com says:

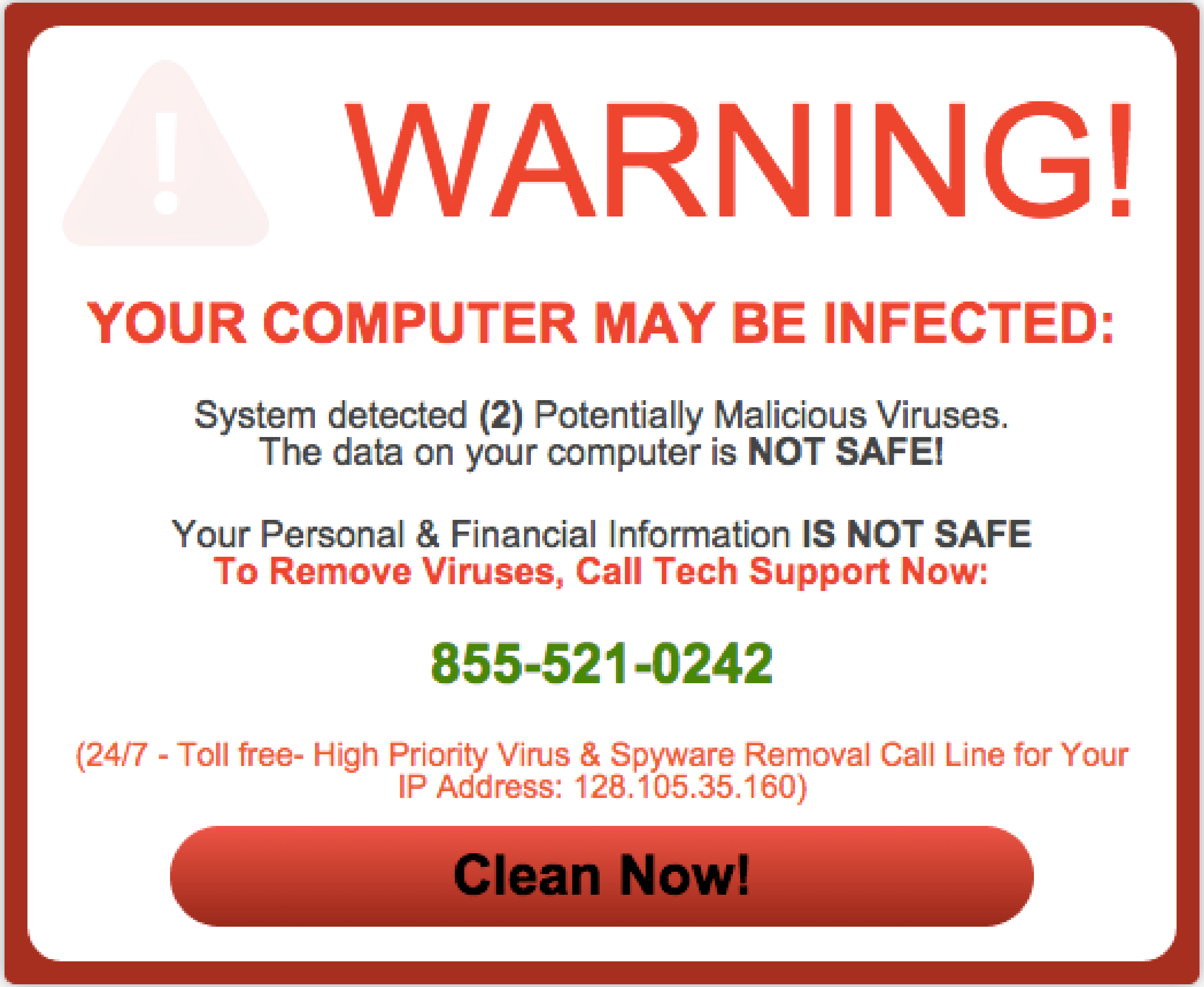
****

Congratulations!

You are Todays Lucky Visitor.

Click OK to continue

****



WARNING!

YOUR COMPUTER MAY BE INFECTED:

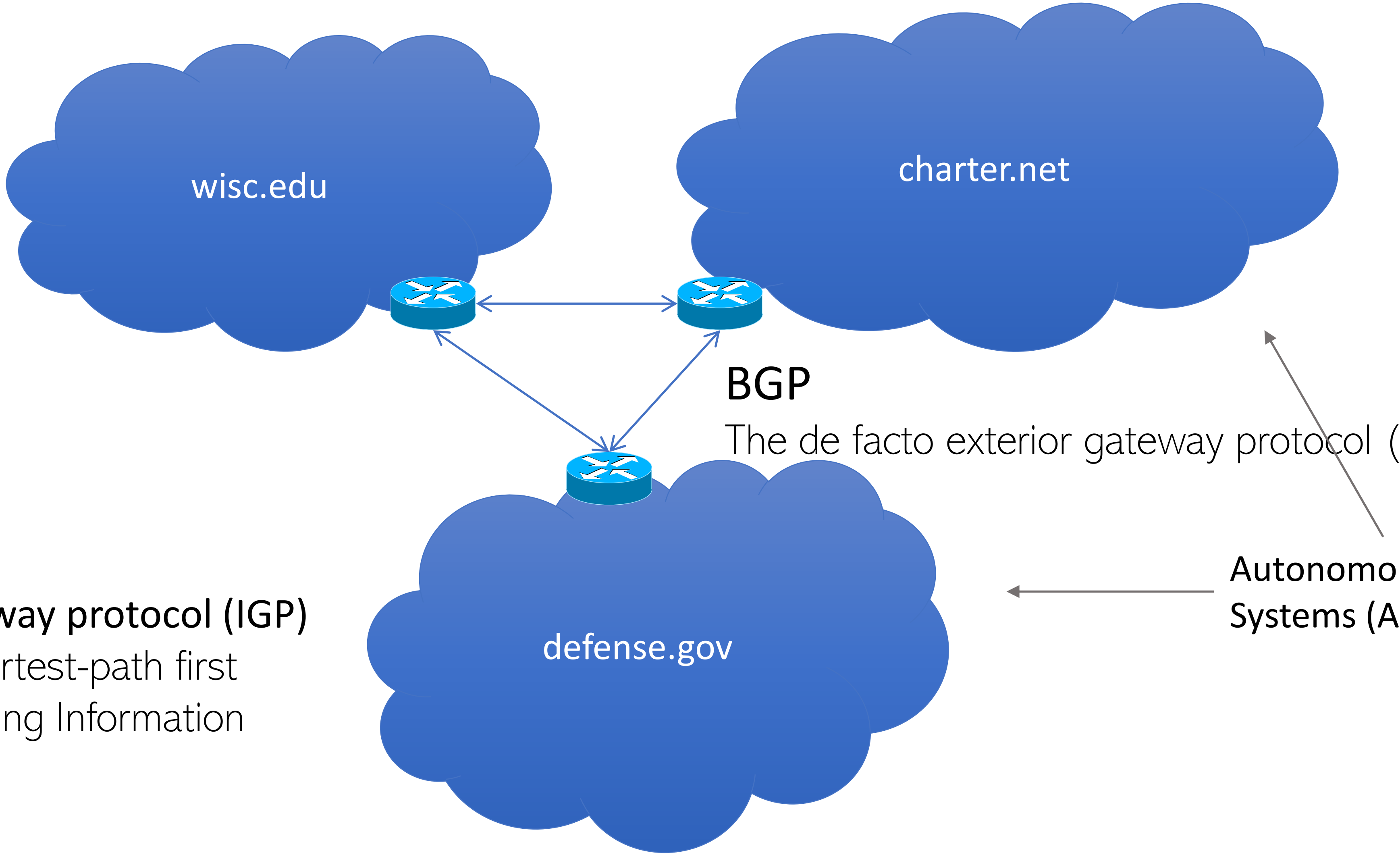
System detected **(2)** Potentially Malicious Viruses.
The data on your computer is **NOT SAFE!**

Your Personal & Financial Information **IS NOT SAFE**
To Remove Viruses, Call Tech Support Now:

855-521-0242

(24/7 - Toll free- High Priority Virus & Spyware Removal Call Line for Your IP Address: 128.105.35.160)

BGP and routing



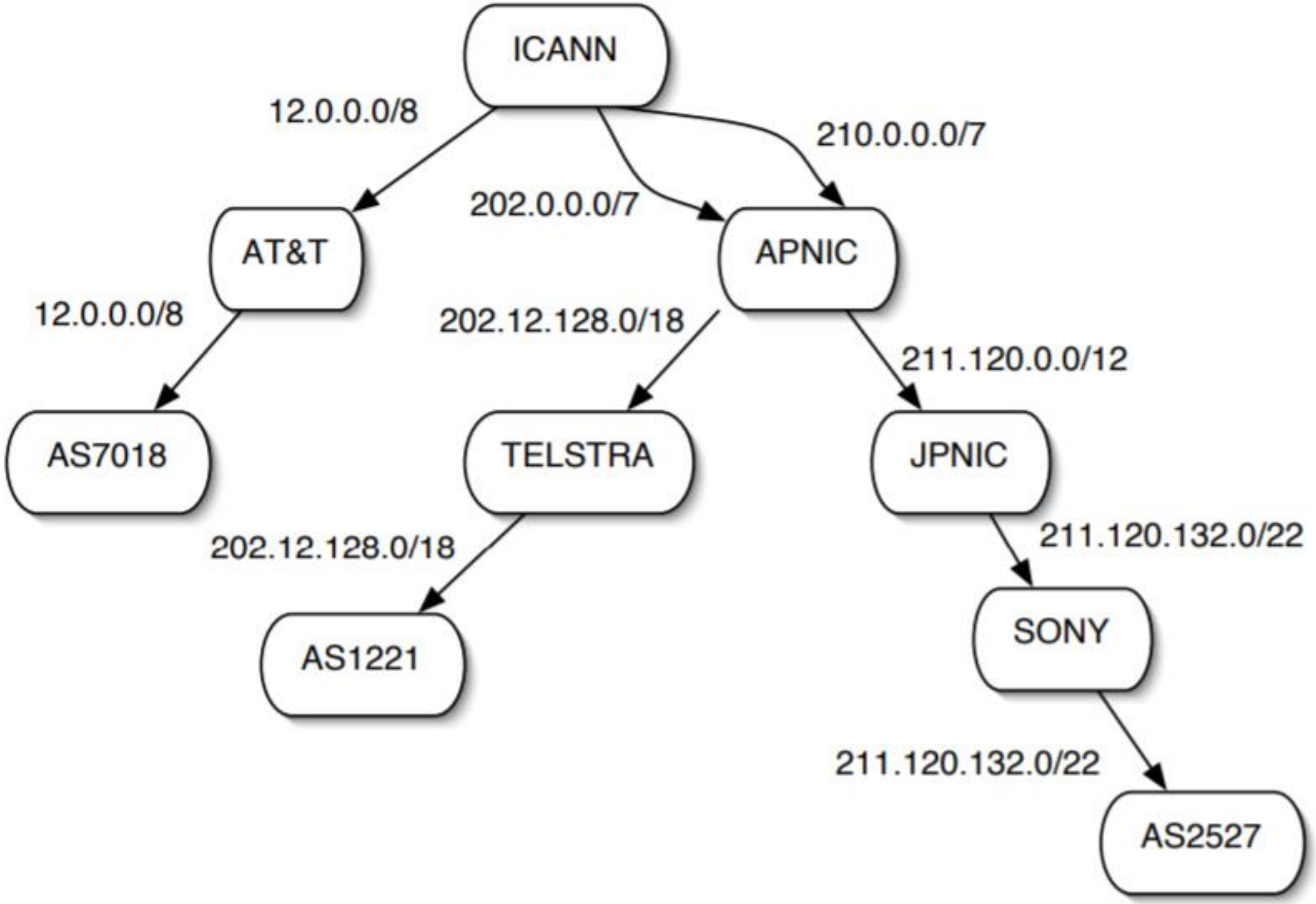
BGP

The de facto exterior gateway protocol (EGP)

Autonomous Systems (AS)

Interior Gateway protocol (IGP)

E.g, Open shortest-path first (OSPF), Routing Information Protocol (RIP)



Source:
http://patrickmcdaniel.org/pubs/td-5ugj33.pdf

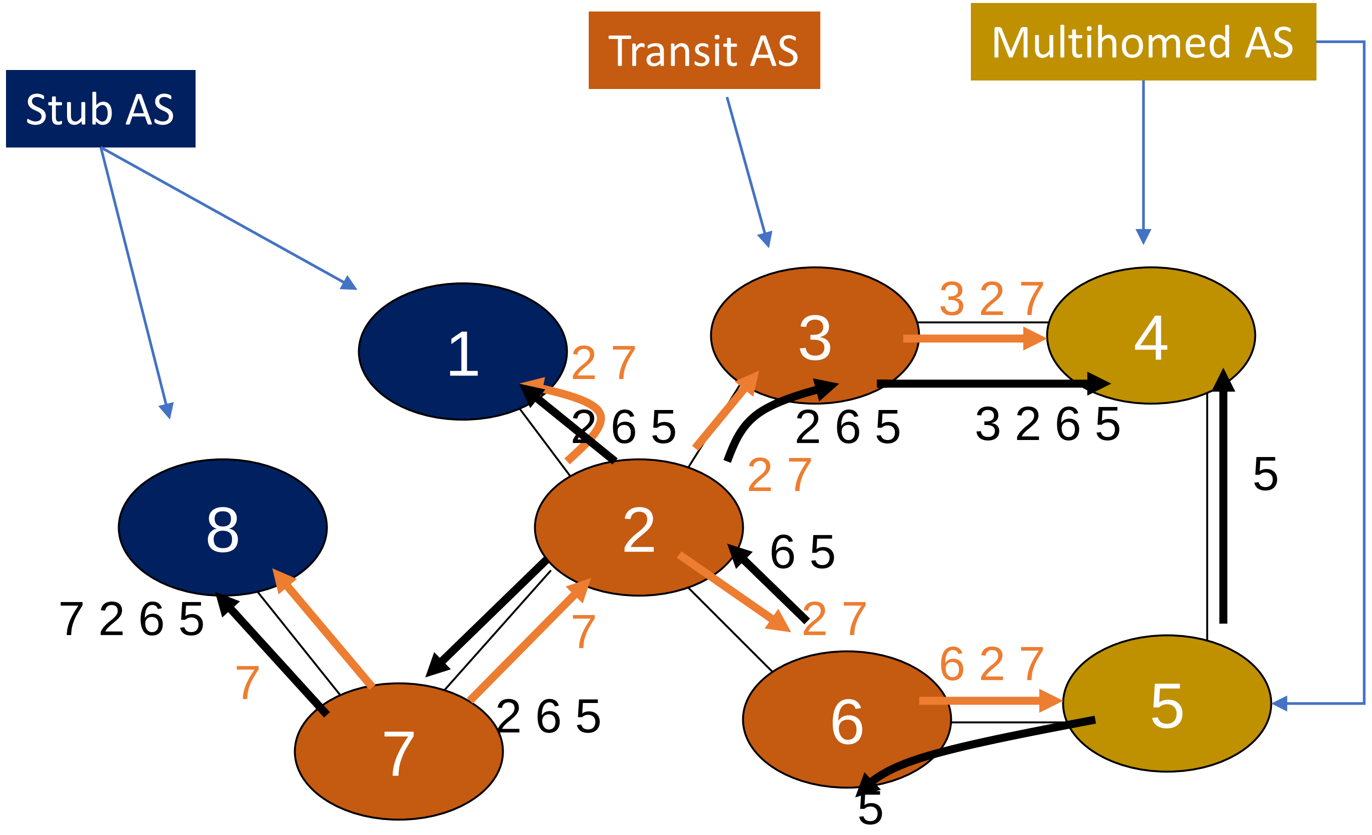
BGP

- Policy-based routing
  - AS can set policy about how to route
    - economic, security, political considerations
- BGP routers use TCP connections to transmit routing information
- Iterative announcement of routes

BGP example

[D. Wetherall]

- Algorithm seems to work OK in practice
  - BGP does not respond well to frequent node outages



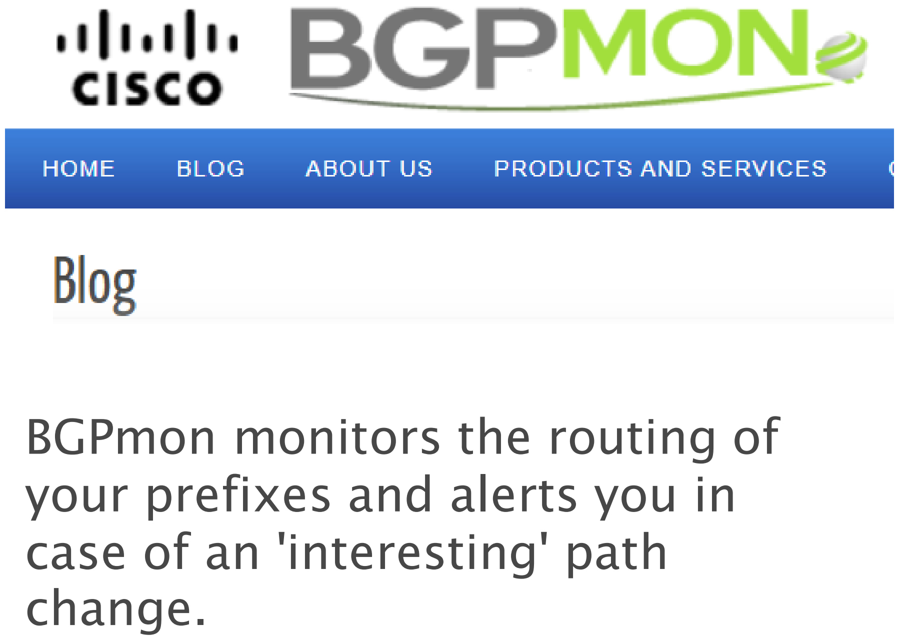
IP hijacking

- BGP is unauthenticated
  - Anyone can advertise any routes
  - False routes will be propagated
- This allows IP hijacking
  - AS announces it originates a prefix it shouldn’t
  - AS announces it has shorter path to a prefix
  - AS announces more specific prefix

Malicious or misconfigurations?

- AS 7007 incident in 1997
  - “Okay, so panic ensued, and we unplugged *everything* at 12:15PM almost to the second.” [sic]
  - http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html
- China Telecom hijacks large chunks of Internet in 2010
  - http://bgpmon.net/blog/?p=282

https://www.bgpmon.net



Blog

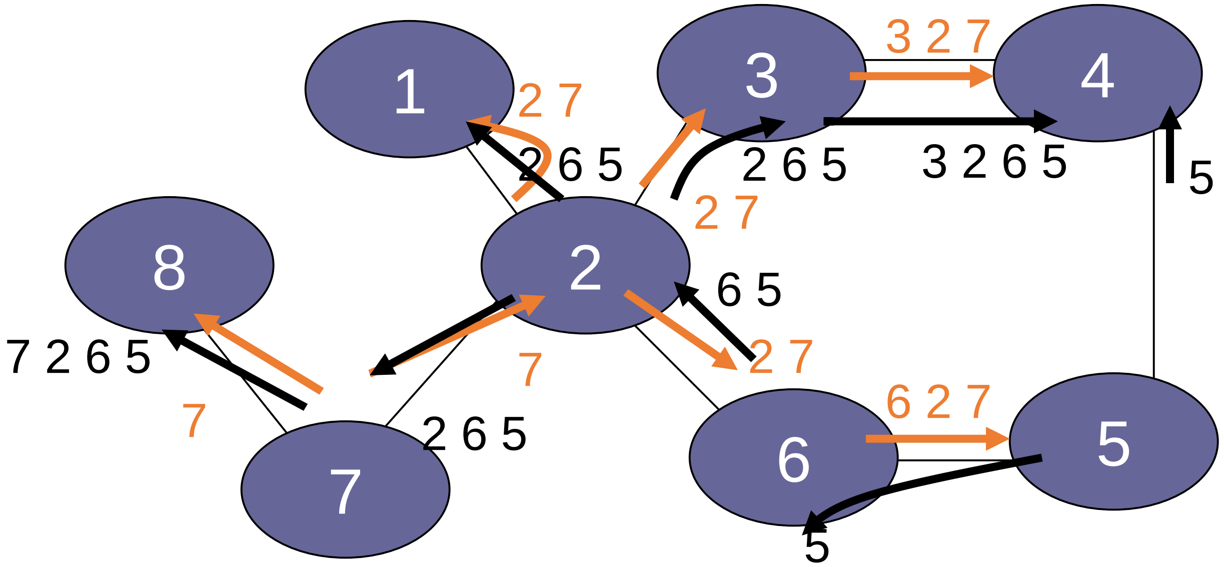
BGPmon monitors the routing of your prefixes and alerts you in case of an 'interesting' path change.

YouTube incident (2008)

- Pakistan attempts to block Youtube
  - youtube is 208.65.152.0/22
  - youtube.com = 208.65.153.238
- Pakistan ISP advertises 208.65.153.0/24
  - more specific, prefix hijacking
- Internet thinks youtube.com is in Pakistan!
- Outage resolved in 2 hours…

BGPsec

[D. Wetherall]



- Route announcements must be cryptographically signed
  - AS can only advertise as itself
  - AS cannot advertise for IP prefixes it does not own
- Requires a public-key infrastructure (PKI)

Deploy360 16 October 2017

BGPSec – A reality now

RFC 8205

Need to wait for ASes to catch up!

Summary: Internet Security

- Recurring themes:
  - Built without any authenticity mechanisms in mind
  - Functionality mechanisms (sequence #'s) become implicit security mechanisms
  - New attempts at (somewhat) backwards-compatible security mechanisms
    - IP -> IPsec
    - DNS -> DNSsec
    - BGP -> BGPsec