Infected ATMs Give Away Millions of Dollars Without Credit Cards

81

Soulskill posted yesterday | from the i'll-order-a-dozen dept.

An anonymous reader writes:

> Kaspersky Lab performed a forensic investigation into cybercriminal attacks targeting multiple ATMs around the world. During the course of this investigation, researchers discovered the Tyupkin malware used to infect ATMs and allow attackers to remove money via direct manipulation, stealing millions of dollars. The criminals work in two stages. First, they gain physical access to the ATMs and insert a bootable CD to install the Tyupkin malware. After they reboot the system, the infected ATM is now under their control and the malware runs in an infinite loop waiting for a command. To make the scam harder to spot, the Tyupkin malware only accepts commands at specific times on Sunday and Monday nights. During those hours, the attackers are able to steal money from the infected machine.

US Says It Can Hack Foreign Servers Without Warrants

280

Soulskill posted 6 hours ago | from the how-to-win-friends dept.

Advocatus Diaboli tips news that the U.S. government is now arguing it doesn't need warrants to hack servers hosted on foreign soil. At issue is the current court case against Silk Road operator Ross Ulbricht. We recently discussed how the FBI's account of how they obtained evidence from Silk Road servers didn't seem to mesh with reality. Now, government lawyers have responded in a new court filing (PDF). They say that even if the FBI had to hack those servers without a warrant, it doesn't matter, because the Fourth Amendment does not confer protection

DNS and BGP

CS642: Computer Security

Professor Ristenpart

http://www.cs.wisc.edu/~rist/

rist at cs dot wisc dot edu

DNS and BGP

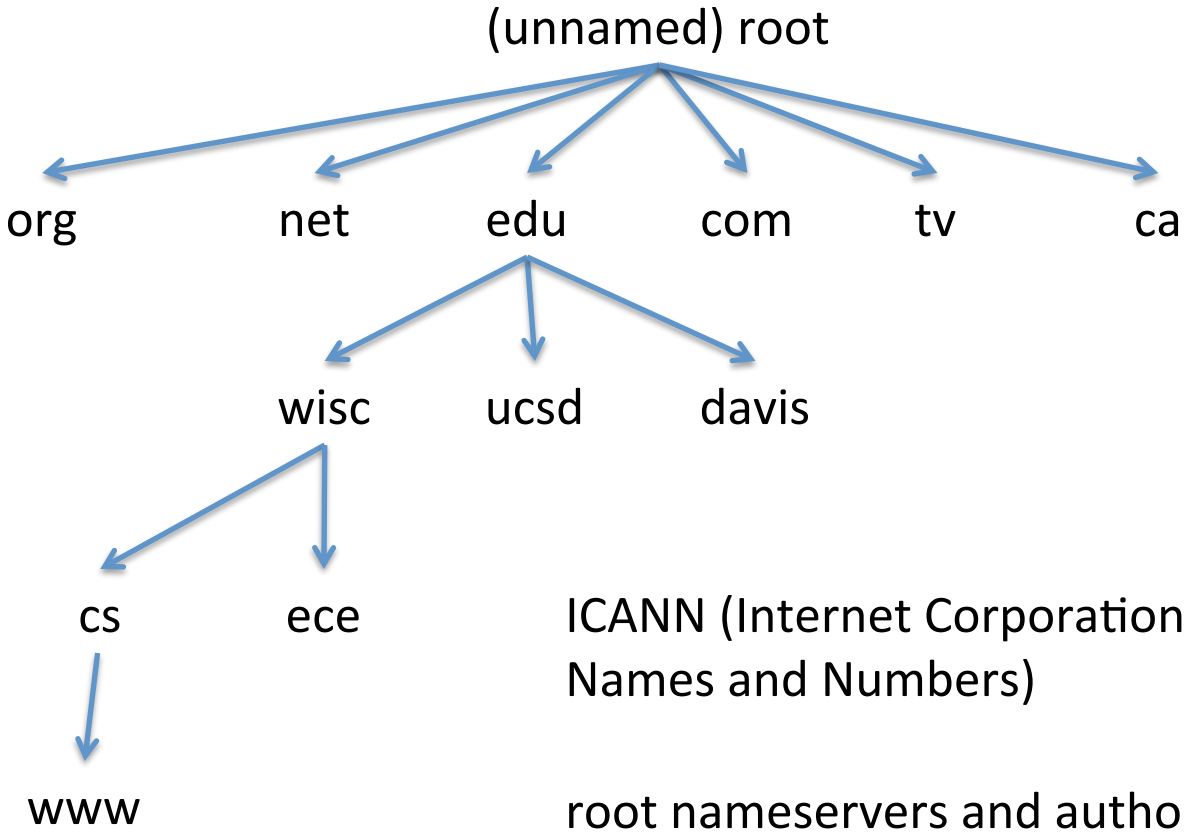
128.105.5.31

We don’t want to have to remember IP addresses

```
[rist@seclab1] (17)$ head hosts
#
#       Wisconsin CS Local Host Table
#
127.0.0.1       localhost
128.105.6.39    smtp.cs.wisc.edu smtp
128.105.6.40    spam.cs.wisc.edu spam spam-test
128.105.6.42    spam.cs.wisc.edu spam spam-test
128.105.6.38    spam.cs.wisc.edu spam spam-test
128.105.1.1     ge-5-1.cisco-border1.cs.wisc.edu ge-5-1.cisco-border1
128.105.1.2     ge-1-2.cisco1.cs.wisc.edu ge-1-2.cisco1
[rist@seclab1] (18)$
```

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

Heirarchical domain name space



Top Level domains (TLD)

Second Level domains

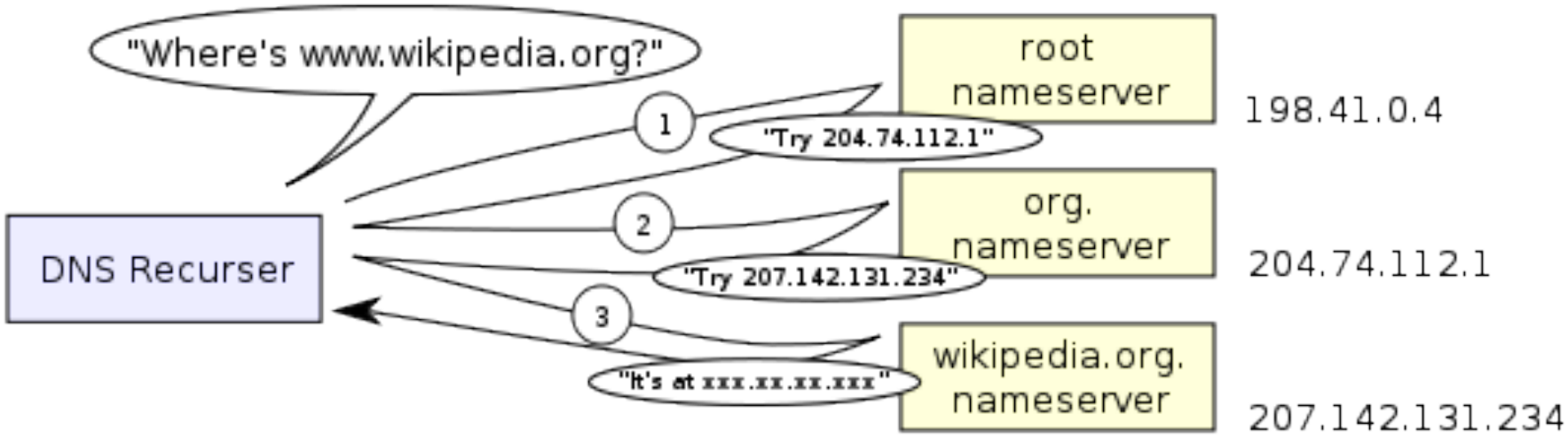
ICANN (Internet Corporation for Assigned Names and Numbers)

root nameservers and authoritative nameservers

Zone: subtree

max 63 characters

Resolving names



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

Example DNS query types

A	address (get me an IPv4 address)
AAAA	IPv6 address
NS	name server
TXT	human readable text, has been used for some encryption mechanisms
MX	mail exchange

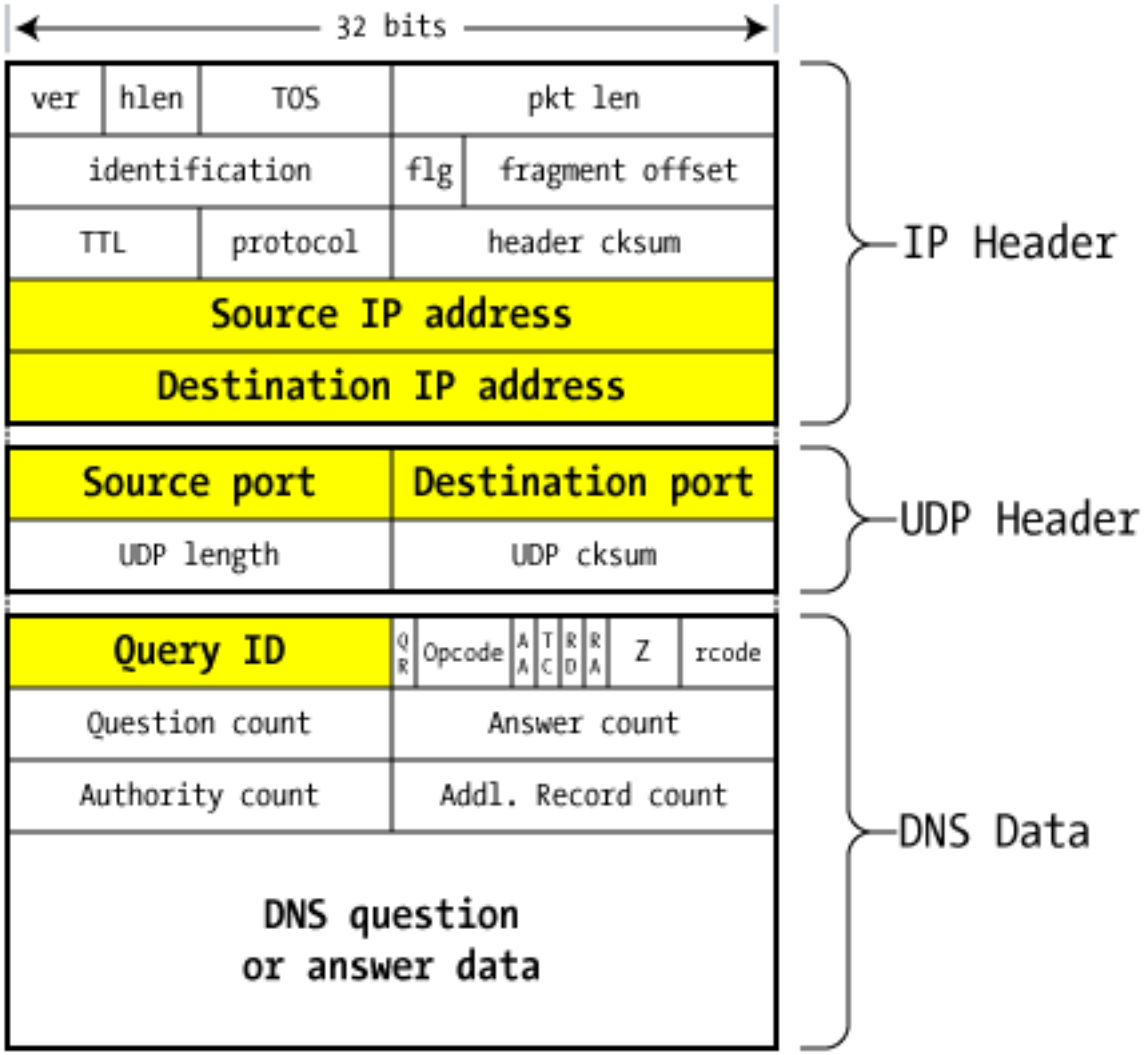
Caching

- 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

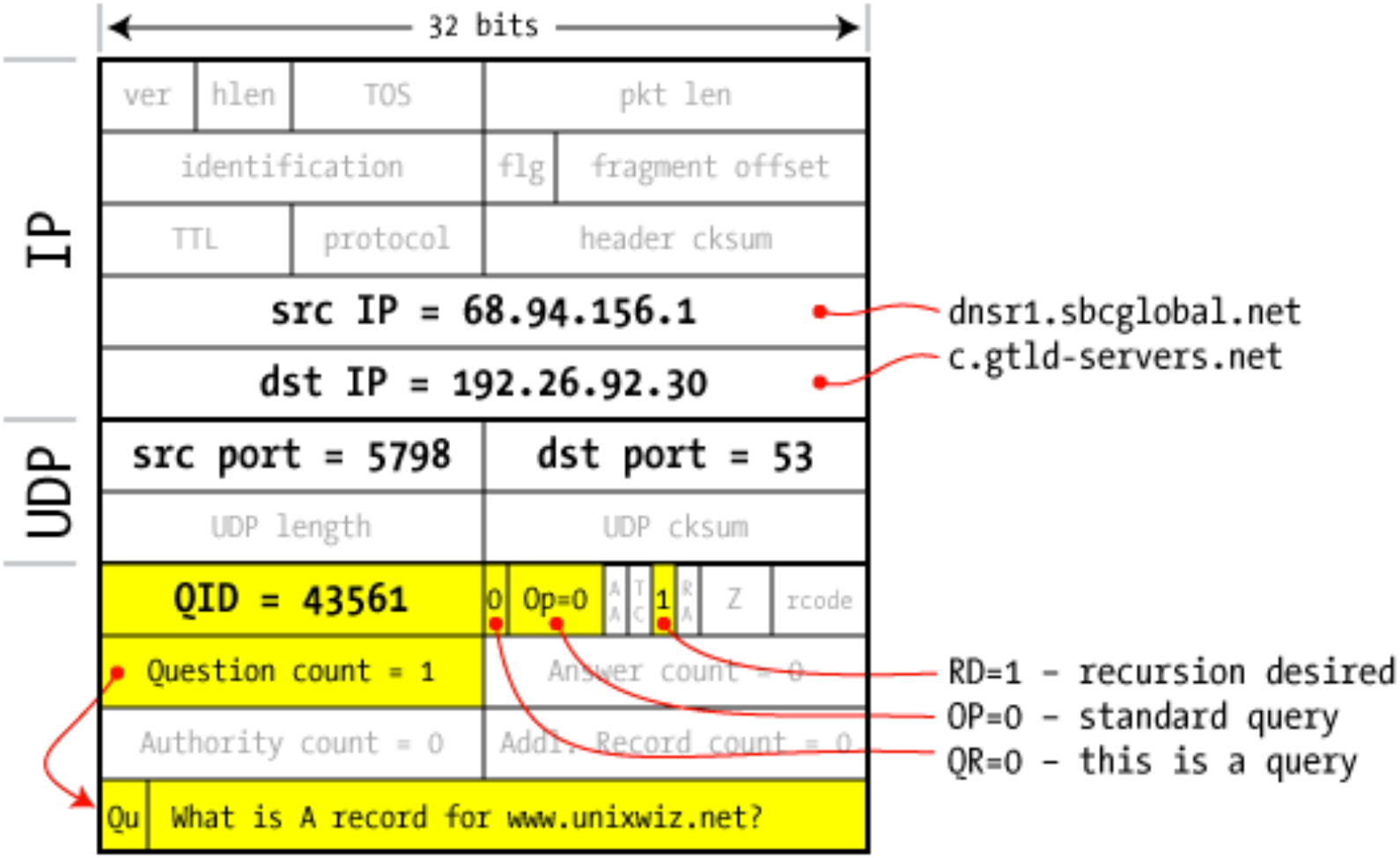
Query ID is 16-bit random value

We'll walk through the example from Friedl's document

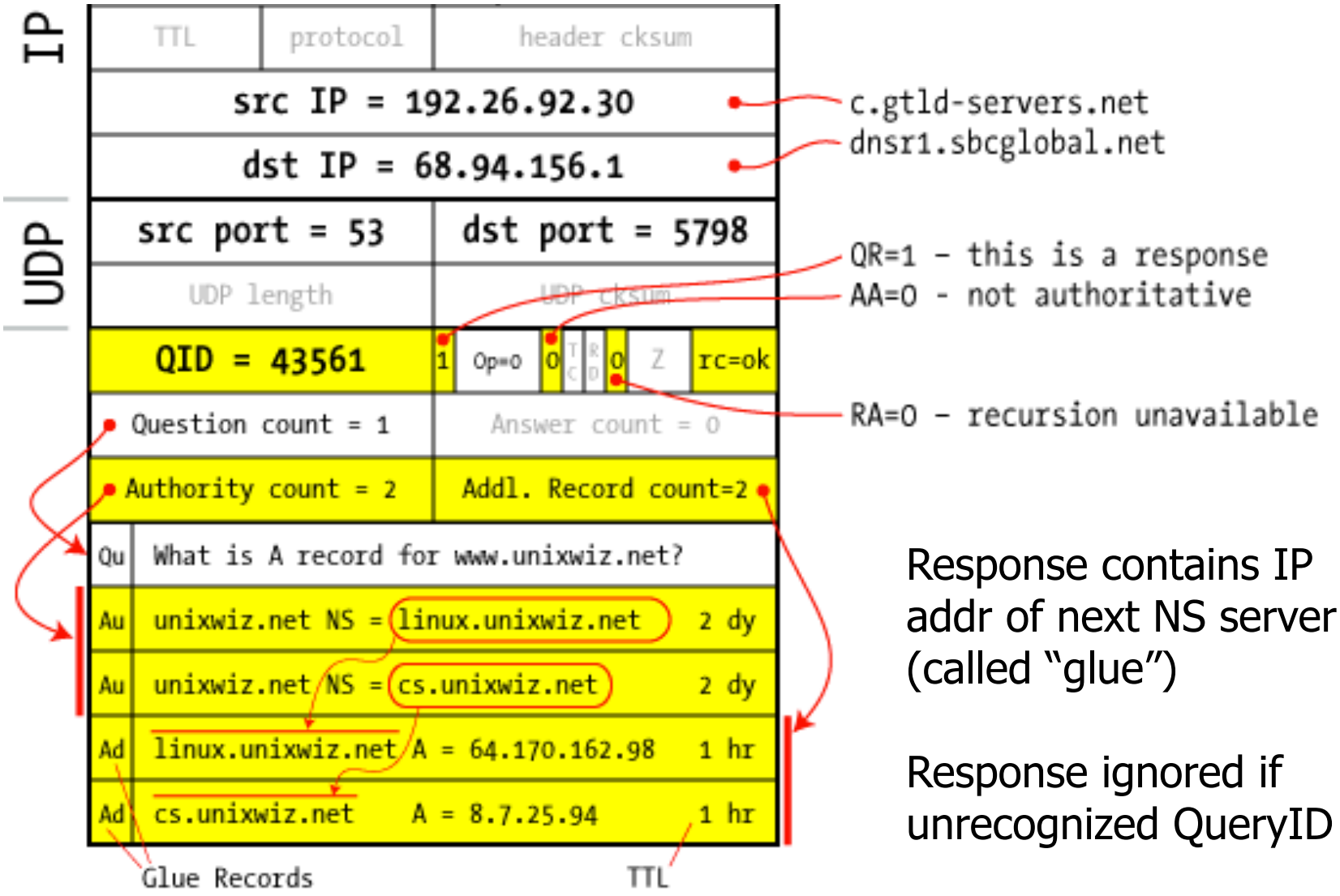


From Friedl explanation of DNS cache poisoning, as are following diagrams

Query from resolver to NS



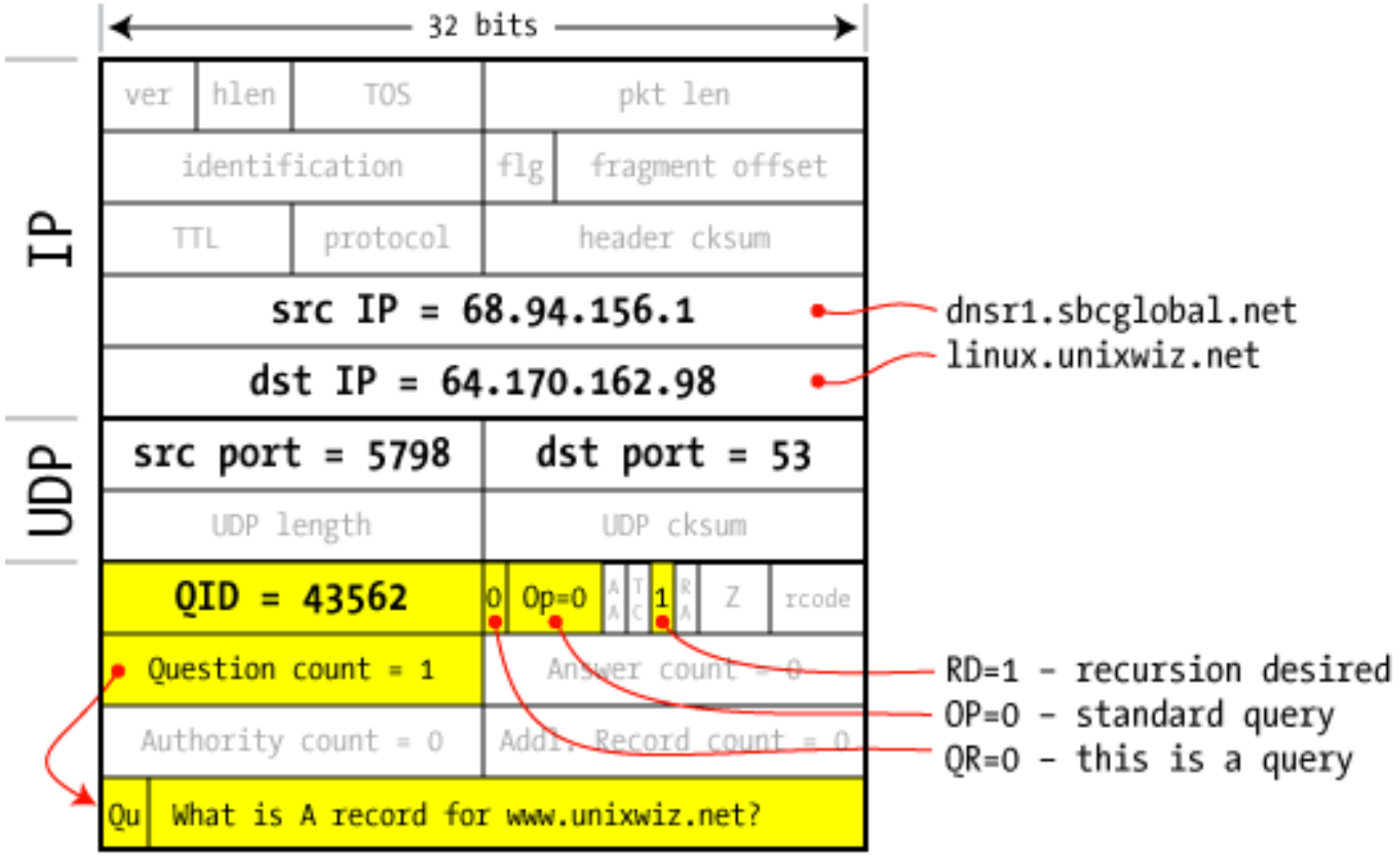
Reply from NS to Resolver



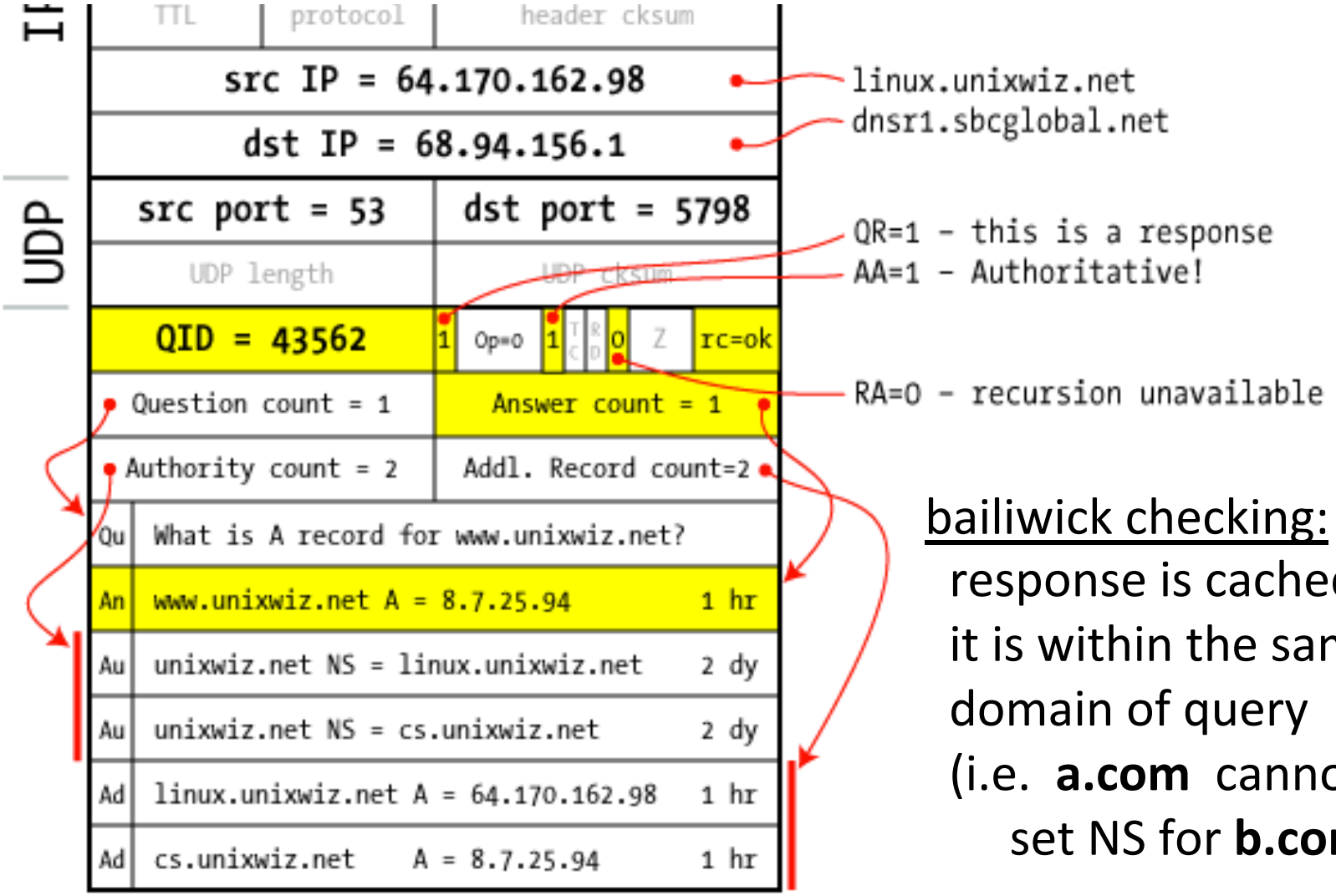
Response contains IP addr of next NS server (called "glue")

Response ignored if unrecognized QueryID

Query to Second NS



Reply from Second NS to Resolver



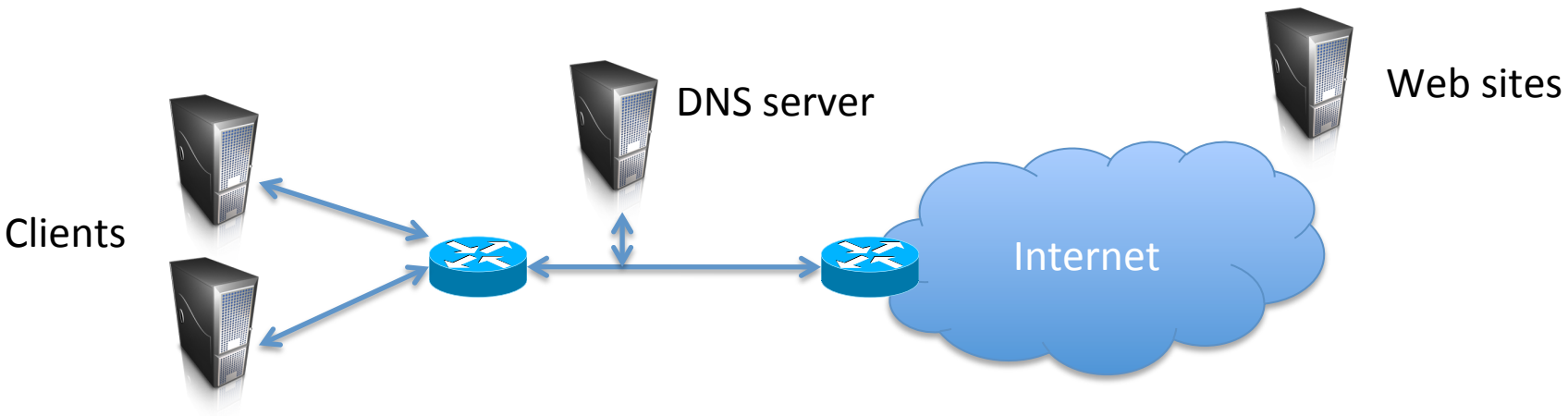
<u>bailiwick checking:</u>

response is cached if it is within the same domain of query (i.e. **a.com** cannot set NS for **b.com**)

Here we go again…

- What security checks are in place?
  - Random query ID's to link responses to queries
  - Bailiwick checking (sanity check on response)
- No authentication
  - DNSsec is supposed to fix this but few DNS servers support it
- Many things trust hostname to IP mapping
  - Browser same-origin policy
  - URL address bar

Attacks against DNS?

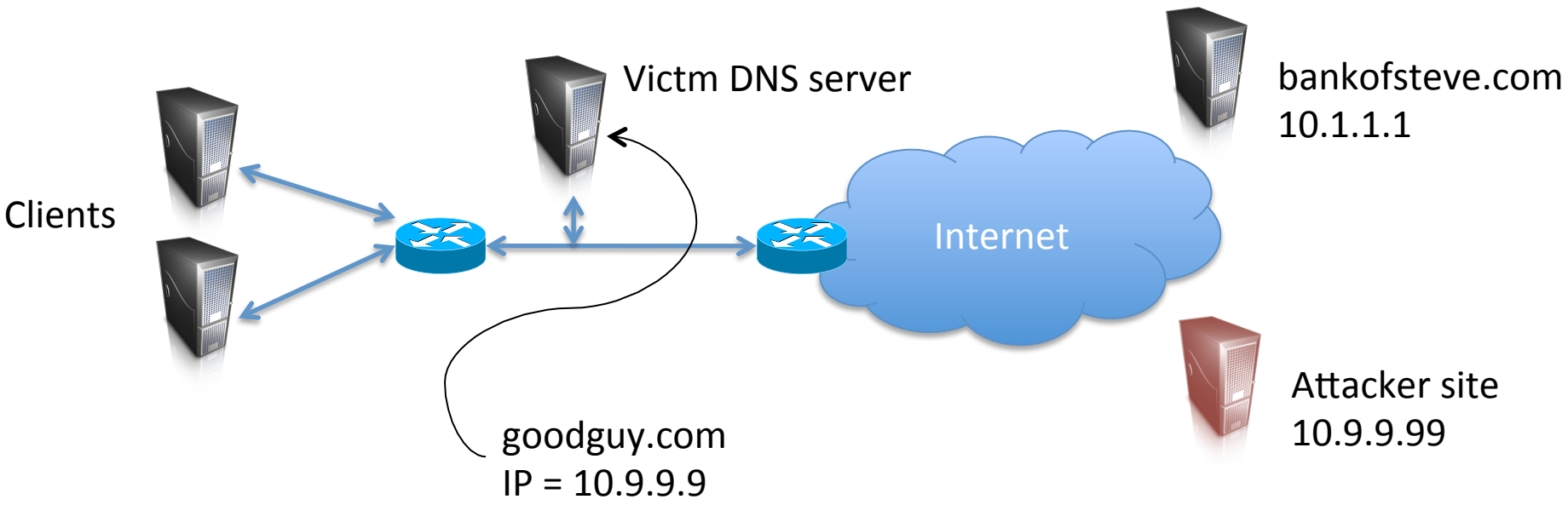


- Corrupted nameservers
- Intercept & manipulate requests
- DDoS
- Cache poisoning
- Phishing / typo squatting / piggy-backing

DDoS against DNS

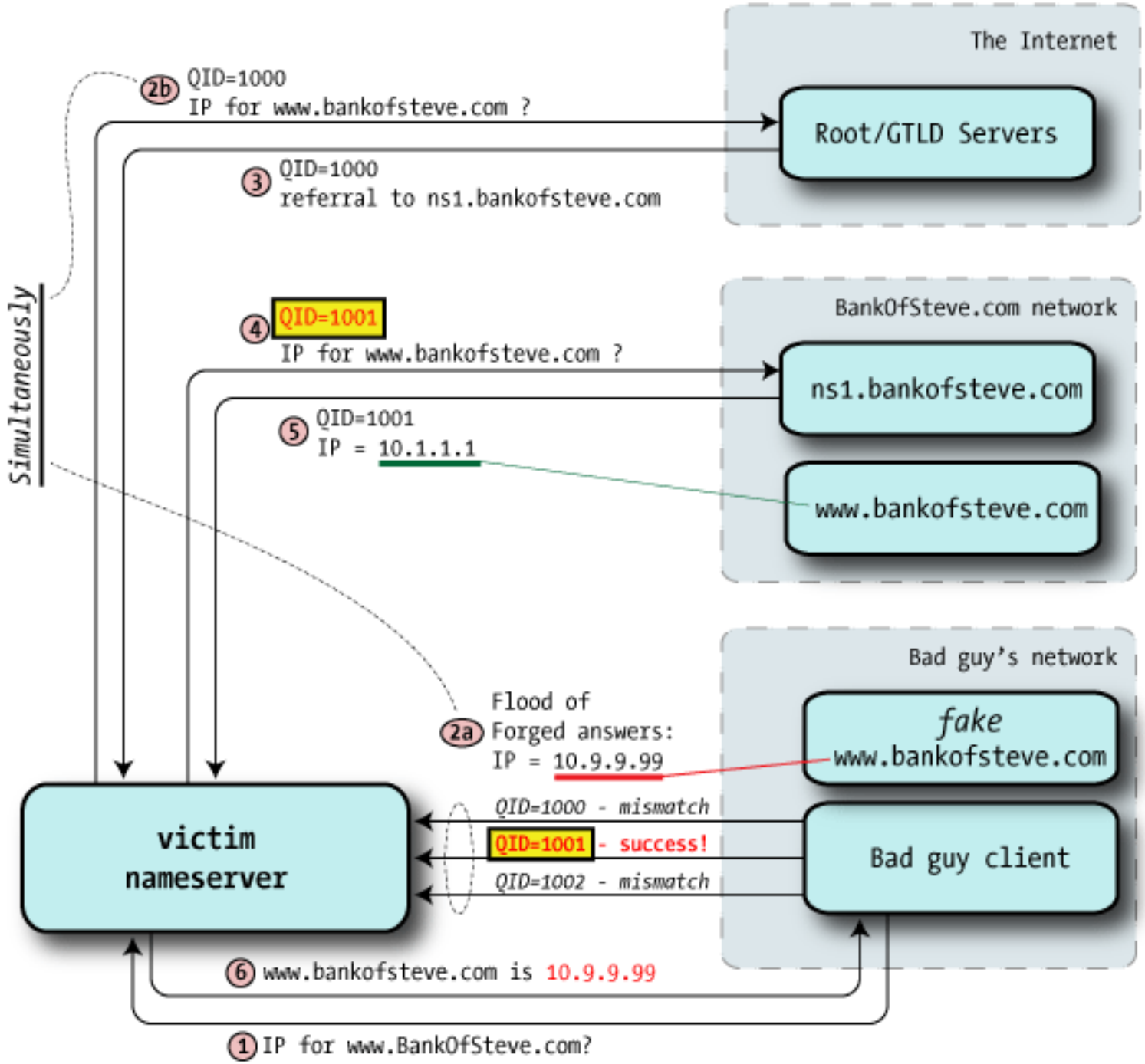
- Denial of Service
  - take down DNS server, clients can't use Internet
  - Feb 6, 2007 attack against 6 of 13 root servers:
    - 2 suffered very badly
    - Others experienced heavy traffic
- DoD purportedly has interesting response:
  - "In the event of a massive cyberattack against the country that 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

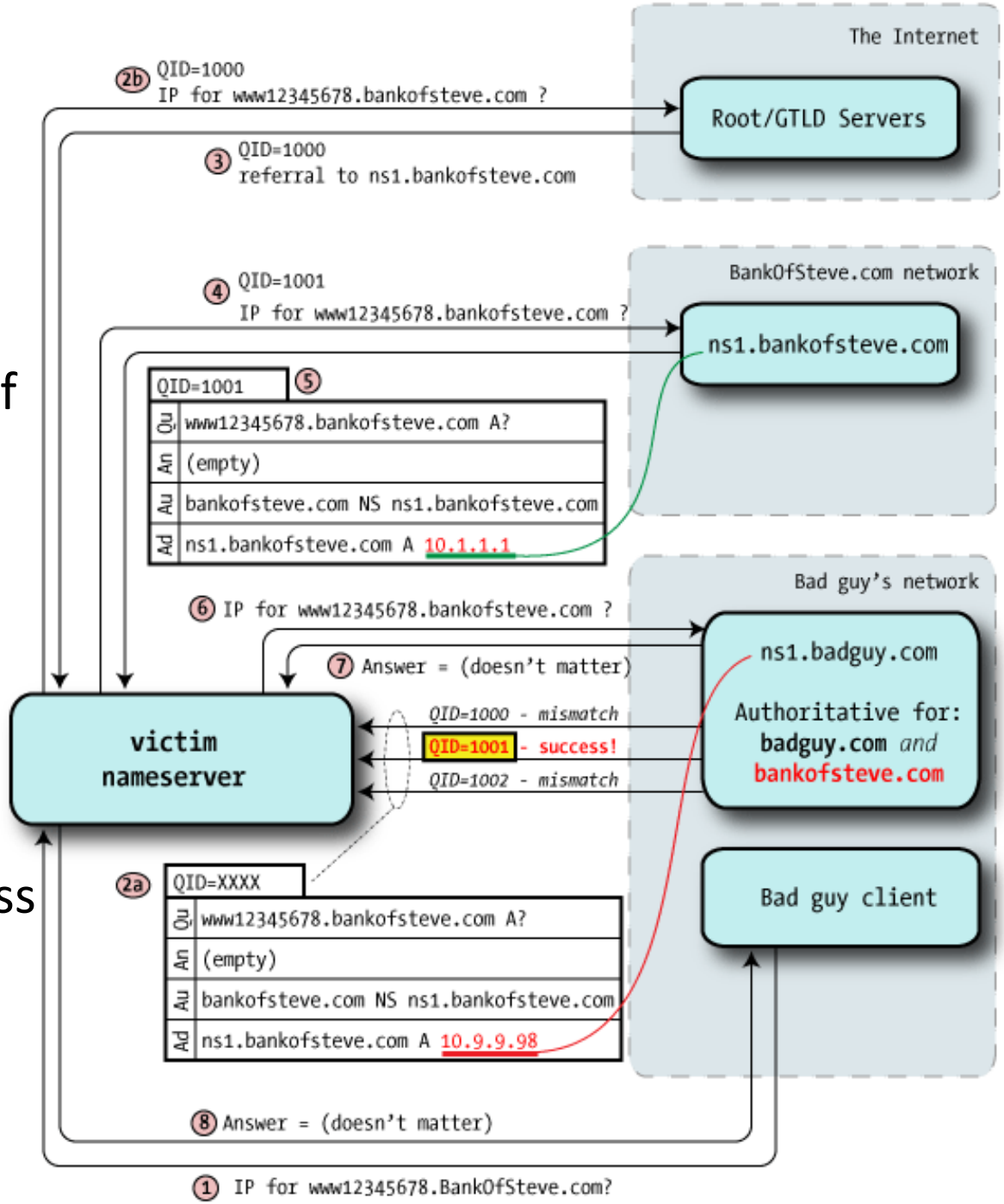

The Internet
Root/GTLD Servers
2b QID=1000
IP for www.bankofsteve.com ?
3 QID=1000
referral to ns1.bankofsteve.com
Simultaneously
BankOfSteve.com network
4 QID=1001
IP for www.bankofsteve.com ?
ns1.bankofsteve.com
5 QID=1001
IP = 10.1.1.1
www.bankofsteve.com
Bad guy's network
Flood of
2a Forged answers:
IP = 10.9.9.99
fake
www.bankofsteve.com
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?

Another idea:

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

How many tries does this require?

- Try 256 different QIDs
- Good chance of success
- Repeat if needed



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 [...]*

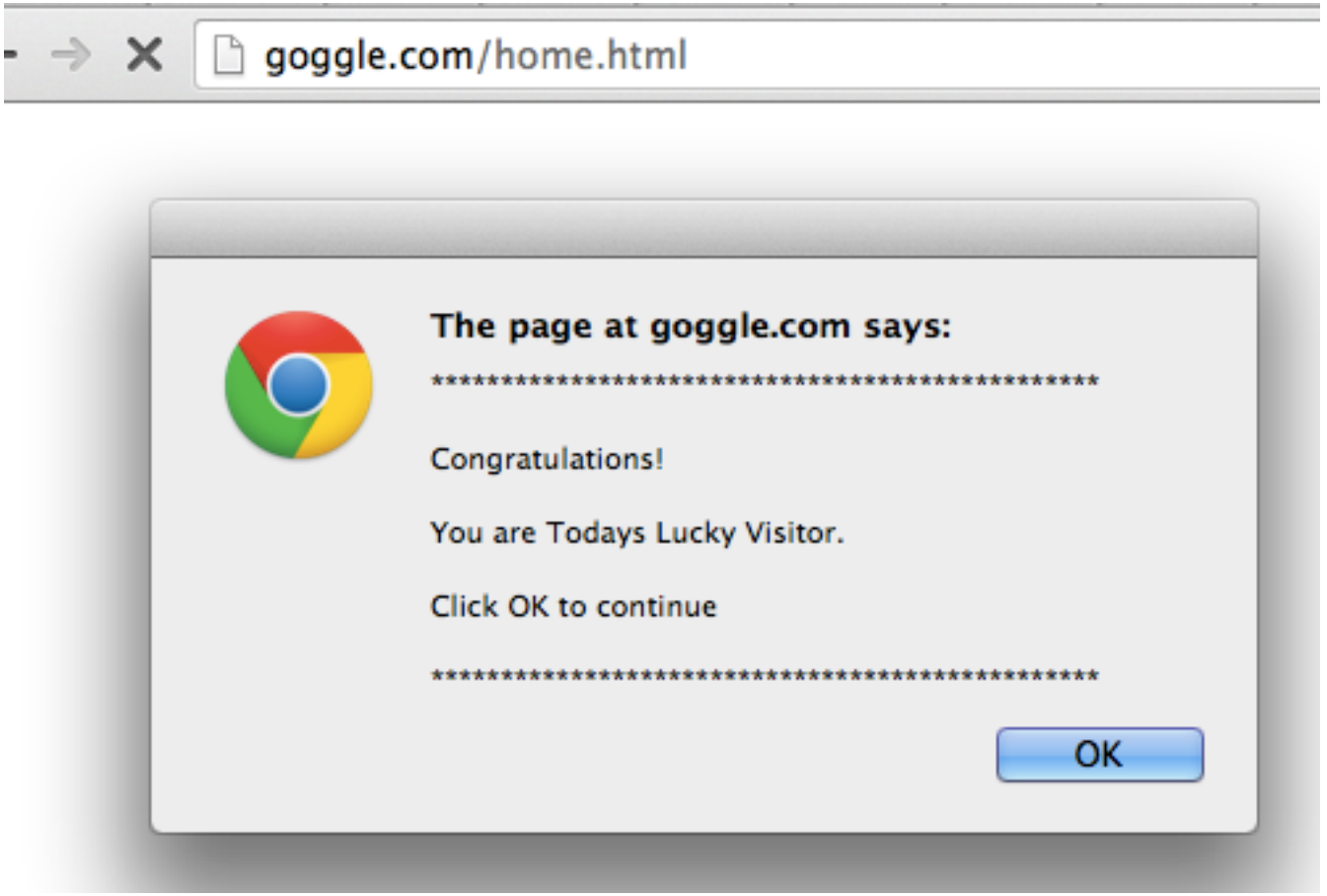
http://www.zdnet.com/blog/security/hd-moore-pwned-with-his-own-dns-exploit-vulnerable-at-t-dns-servers-to-blame/1608?tag=content;siu-container

Defenses

- Query ID size is fixed at 16 bits
- Repeat each query with fresh Query ID
  - Doubles the space
- Randomize UDP ports
- DNSsec
  - Cryptographically sign DNS responses, verify via chain of trust from roots on down

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
****
OK


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)
Clean Now!

SEO Via DNS "Piggybacking"

Posted by samzenpus on Wednesday October 12, @04:03PM
from the slip-in-there dept.

An anonymous reader writes

> "There is an interesting story over at the SANS Internet Storm Center that shows details on about 50 organizations that have had new machine names added to their DNS zone information. These were then pointed to sites used to boost the search engine cred of pharma, personals, and porn sites. If you outsource your DNS, how would you ever catch something like this?"

Read the **67** comments

fraud seo it

DNS piggybacking

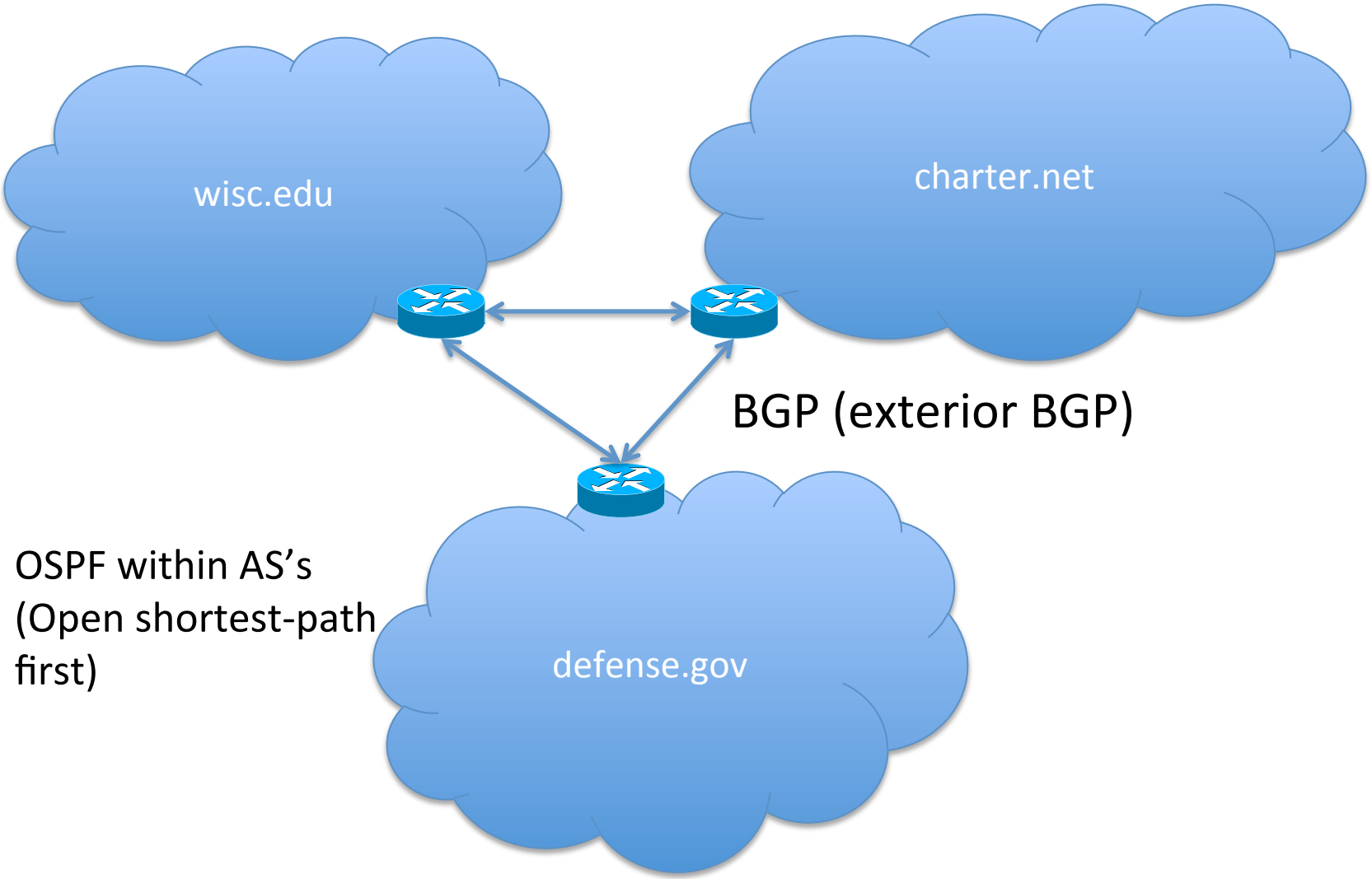
Piggy backed sites	IP	Main site	IP
buy-cialis.sacmetrofire.ca.gov	74.220.215.210	www.sacmetrofire.ca.gov	66.147.240.176
buy-viagra.sacmetrofire.ca.gov			
drugs.sacmetrofire.ca.gov			
mgdrugs.sacmetrofire.ca.gov			
rxdrugs.sacmetrofire.ca.gov			

From https://isc.sans.edu/diary/What+s+In+A+Name+/11770

Attackers maliciously added extra lower level domain names to valid domain name

This is helpful for search engine optimization

BGP and routing

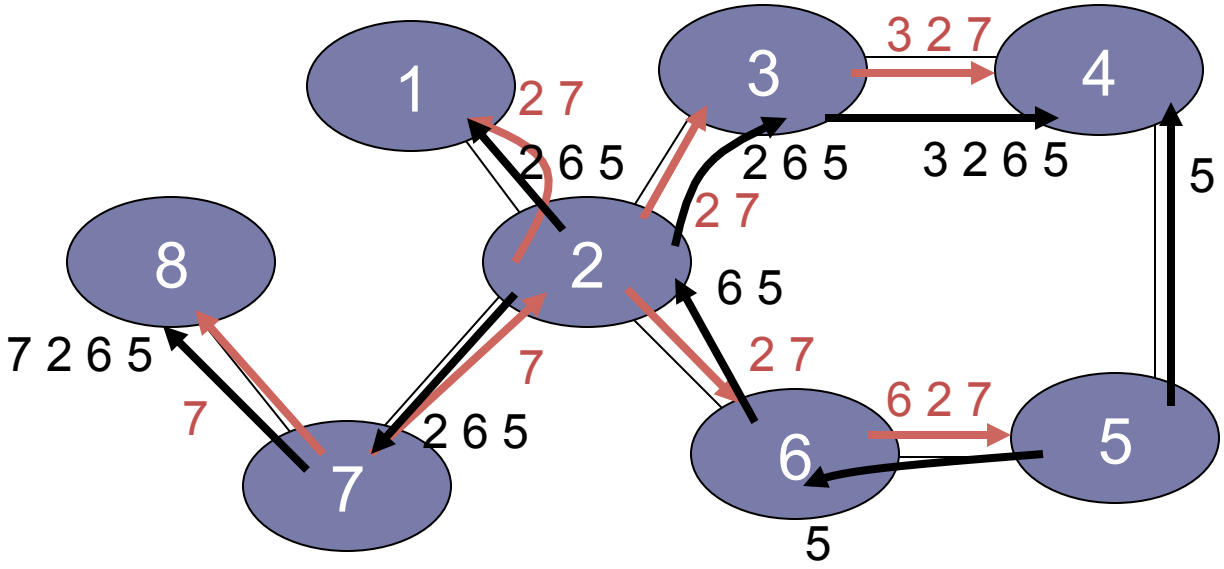


BGP

- 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]



- 2, 7, 3, 6 are Transit AS
- 8, 1 are Stub AS
- 4,5 multihomed AS
- Algorithm seems to work OK in practice
  - BGP does not respond well to frequent node outages

IP hijacking

- BGP 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?

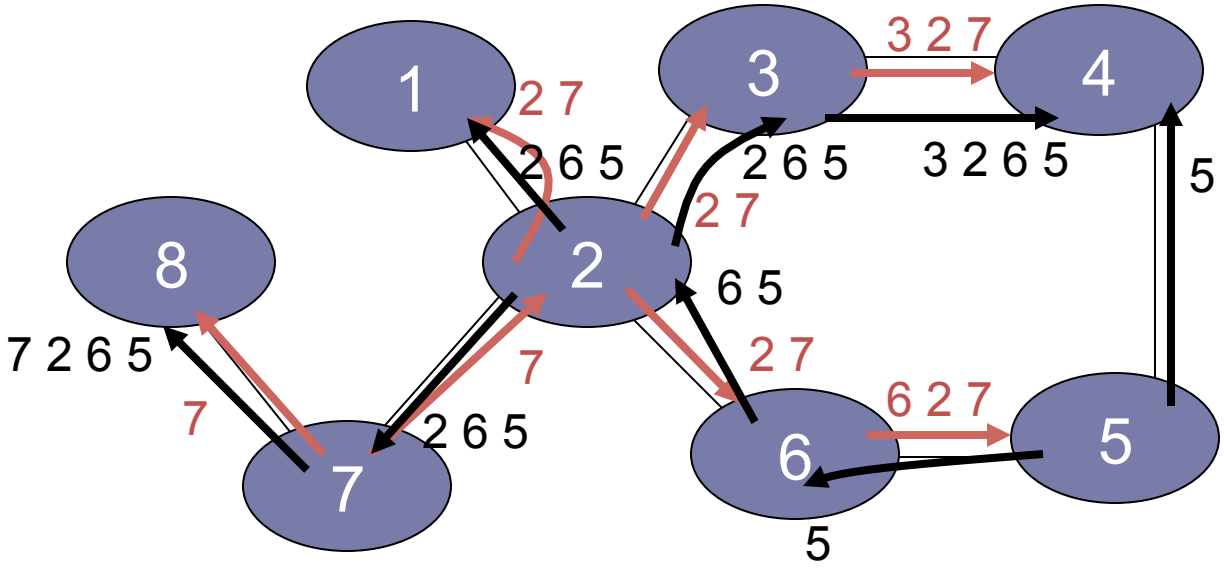
- AS 7007 incident in 1997
  - "Okay, so panic ensued, and we unlugged *everything* at 12:15PM almost to the second." [sic]
  - http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html
- China Telecom hijacks large chunks of Internet in 2010
  - http://bgpmon.net/blog/?p=282

Youtube incident

- 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)
- Still in development:
  - http://tools.ietf.org/html/draft-lepinski-bgpsec-protocol-00#ref-7

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