# CSE 127: Intro to Computer Security

WI24

Lecture 11 - Network Attacks

Slide Credit: Stefan Savage, Deian Stefan, David wagner, Nick weaver, Nadia Heninger, Earlence Fernandes, Imani Munyaka

# Announcements

HW/PA3 - available, start now

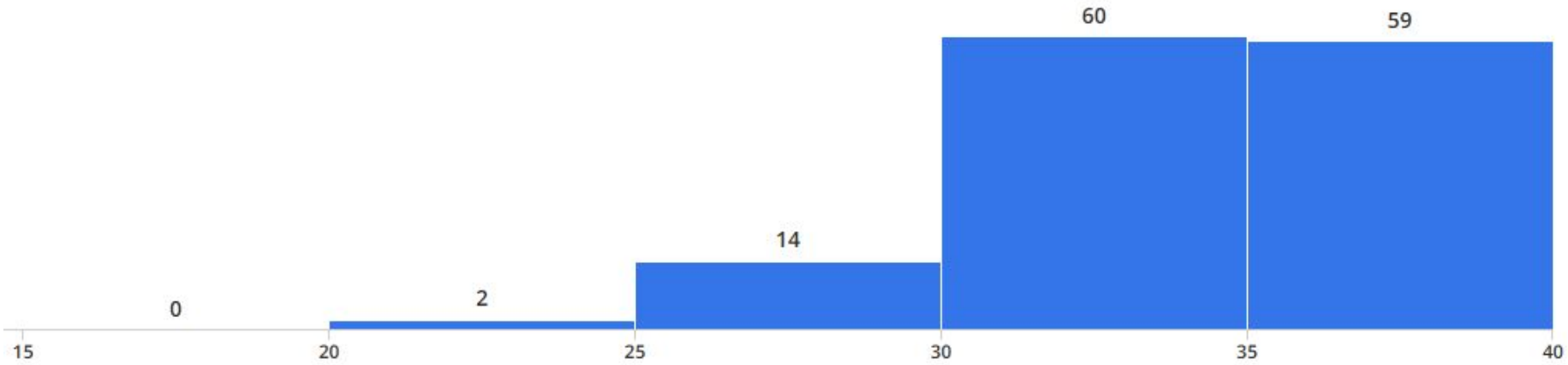
Discussion Session will be held as Autograder Office Hours this week

Async Class on 2/22/24

HW/PA2 Grades Released Tomorrow

Complete Feedback survey linked in announcement

# Midterm Results



# Threat modeling for network attacks

Basic security goals:

- **Confidentiality:** No one should be able to read our data/communications unless we want them to.
- **Integrity:** No one can manipulate our data/communications unless we want them to.
- **Availability:** We can access our data/communication capabilities when we want to.

# Threat modeling for network attacks

Attacker capabilities:

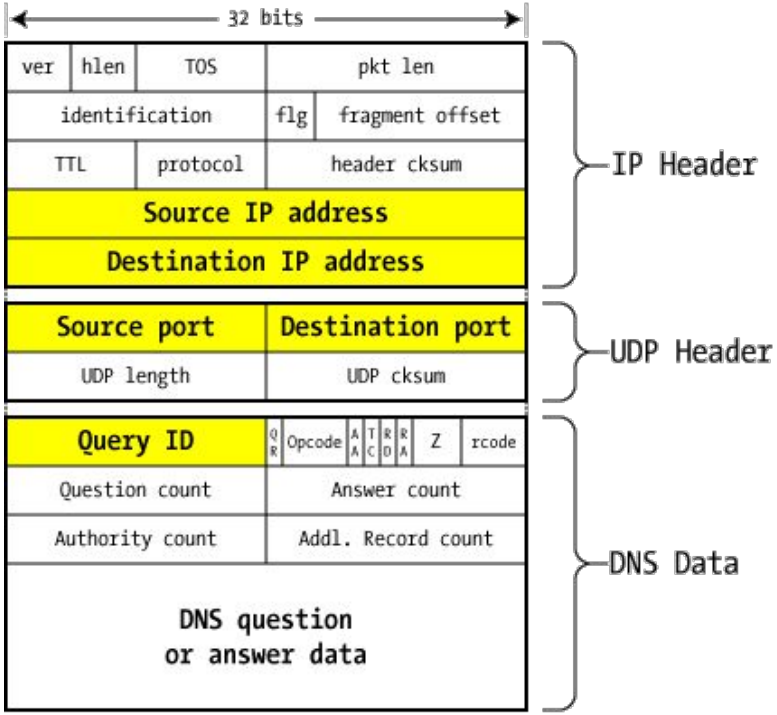
- **Physical access:** Attacker has physical access to the network infrastructure.
- **In path/Man in the middle:** Attacker can see, add, and block packets.
- **On path/Man on the side:** Attacker can see and add packets, but cannot block packets.
- **Passive:** Attacker can see victim's network traffic, but cannot add or modify packets.
- **Off path:** Attacker cannot see network traffic of the victim.

# Different attacks at different layers

| |
|---|
| Application |
| Transport |
| Network |
| Data Link |
| Physical |

- DNS, HTTP, HTTPS
- TCP, UDP
- IP, BGP
- Ethernet, WiFi, ARP
- Physical wires, photons, RF modulation

# Brief Review




*DNS packet on the wire*

DNS - Domain Name System

Query ID - his is a unique identifier created in the query packet that's left intact by the server sending the reply: it allows the server making the request to associate the answer with the question.

QR - 0 (query by client), 1 (response from server)

# Application layer threats: DNS spoofing

Recall:

- DNS maps between domain names and IP addresses.
- Responses cached to avoid query times.

DNS Threat Models:

- **Malicious DNS server:** Any DNS server in query chain can lie about responses.

# Application layer threats: DNS spoofing

Recall:

- DNS maps between domain names and IP addresses.
- Responses cached to avoid query times.

DNS Threat Models:

- **Malicious DNS server:** Any DNS server in query chain can lie about responses.
- **Local/on-path attacker**: Can impersonate DNS server and send a fake response.

# Application layer threats: DNS spoofing

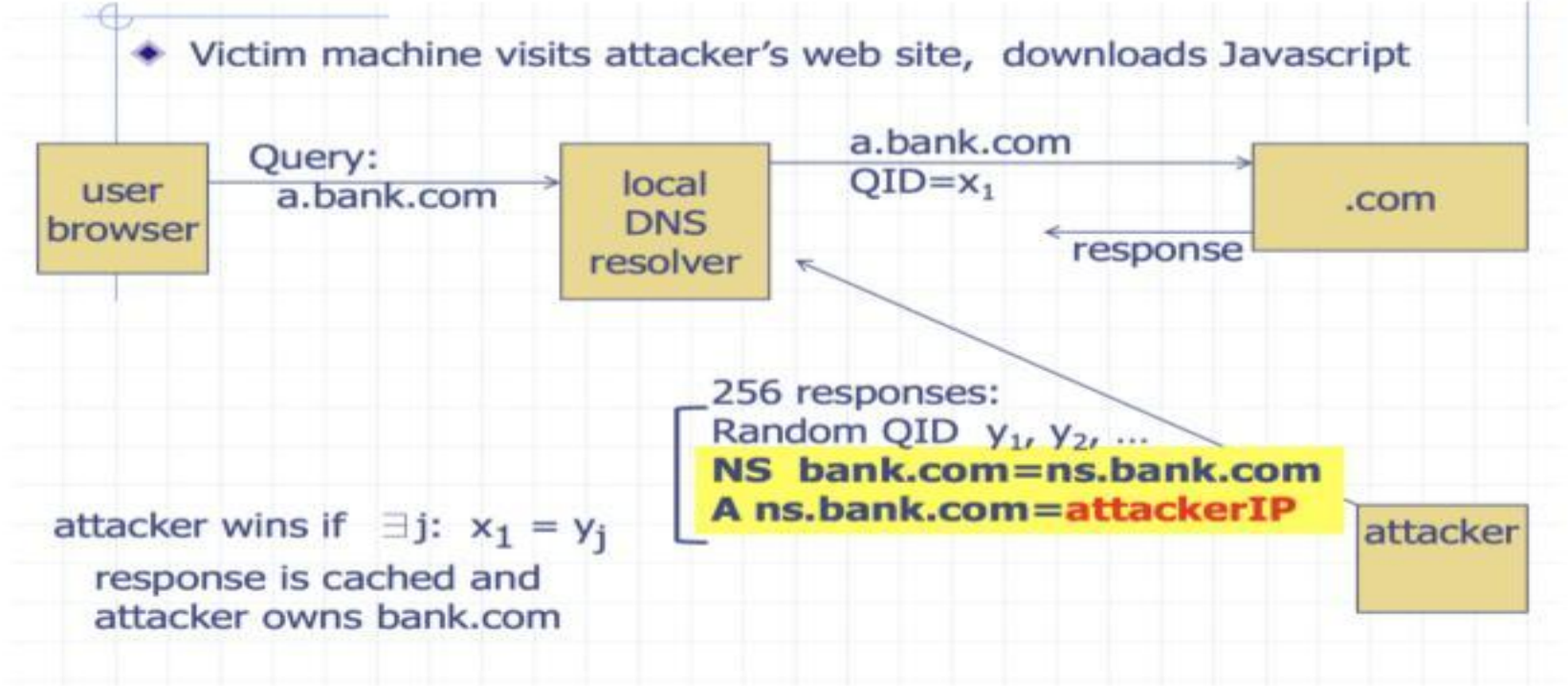
Recall:

- DNS maps between domain names and IP addresses.
- Responses cached to avoid query times.

DNS Threat Models:

- **Malicious DNS server:** Any DNS server in query chain can lie about responses.
- **Local/on-path attacker**: Can impersonate DNS server and send a fake response.
- **Off-path attacker:** Can try to forge response: needs to match 16-bit query ID.
    - Original spec: query ID increments with each request.
    - How can you attack this?

# DNS spoofing: 2008 Kaminsky attack



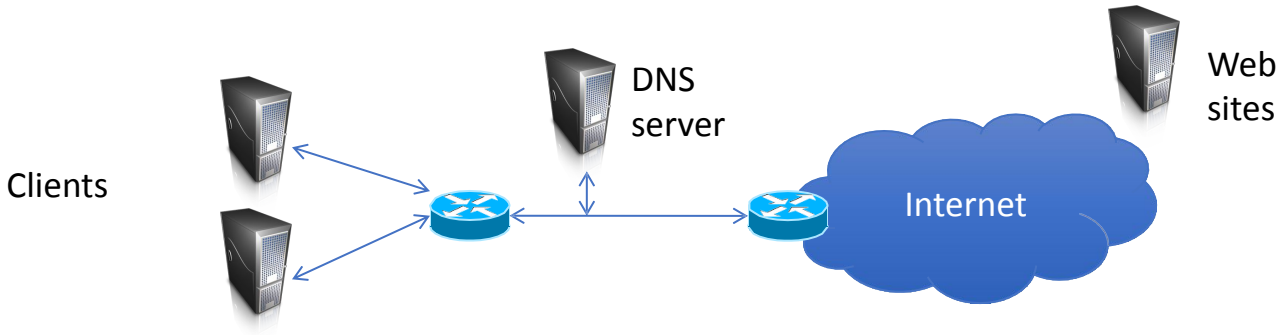

Birthday bound: attacker expects to succeed after $2^8 = 256$ lookups

Mitigation: randomize source port

# (U) New Hotness

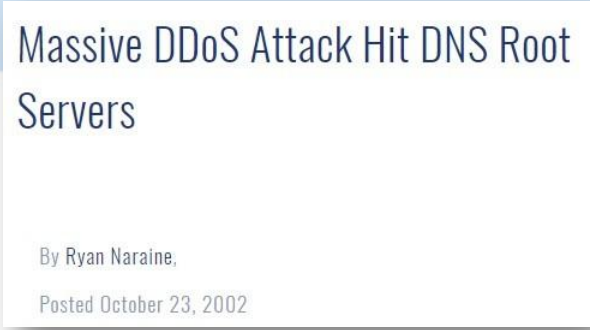
- (TS//SI//REL) QUANTUMBISCUIT
  - Redirection based on keywork
  - Mostly HTML Cookie Values
- (TS//SI//REL) QUANTUMDNS
  - DNS Hijacking
  - Caching Nameservers
- (TS//SI//REL) QUANTUMBOT2
  - Combination of Q-BOT/Q-BISCUIT for web based Command and controlled botnets

# Attacks against DNS?




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

# DDoS against DNS


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 ▼

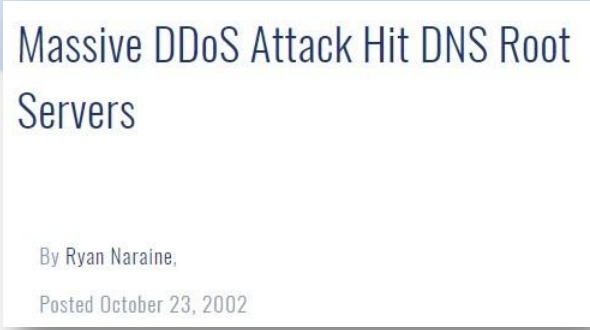
- Denial of Service
  - attacker leverages the functionality of open DNS resolvers in order to overwhelm a target server or network with an amplified amount of traffic, rendering the server and its surrounding infrastructure inaccessible (cloudflare)
  - exploit a disparity in bandwidth consumption (cloudflare)
- 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

# 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?

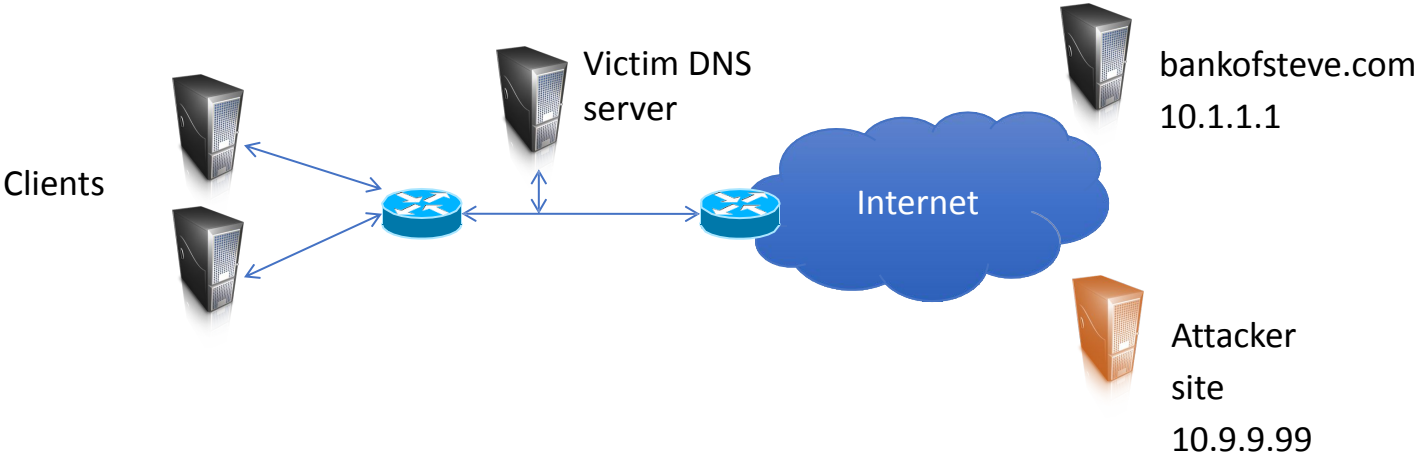
By Kieren McCarthy in San Francisco 8 Dec 2015 at 23:10 27 SHARE ▼

- 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

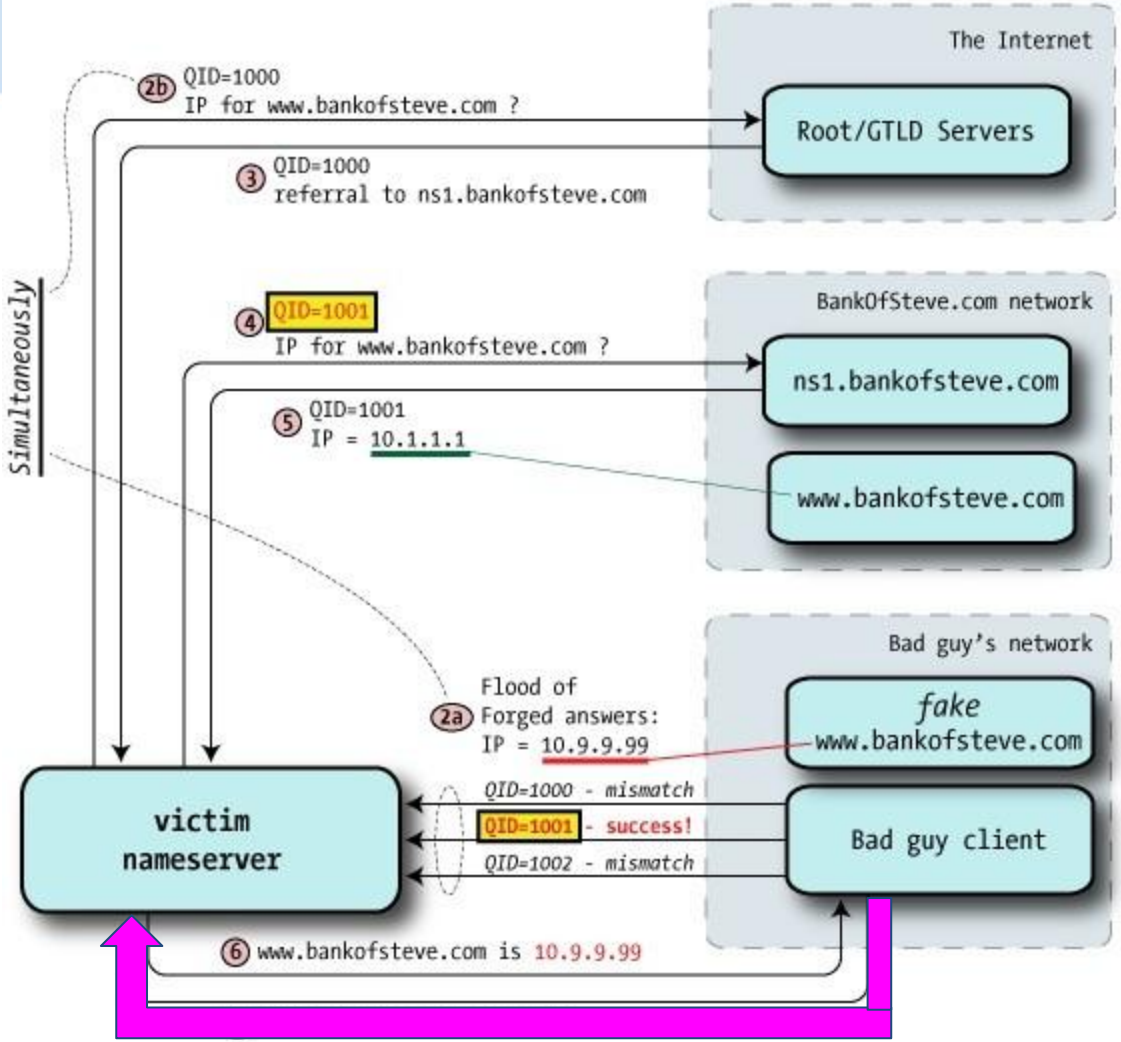
# DNS cache poisoning




How might an attacker do this?

Assume DNS server uses predictable UDP port

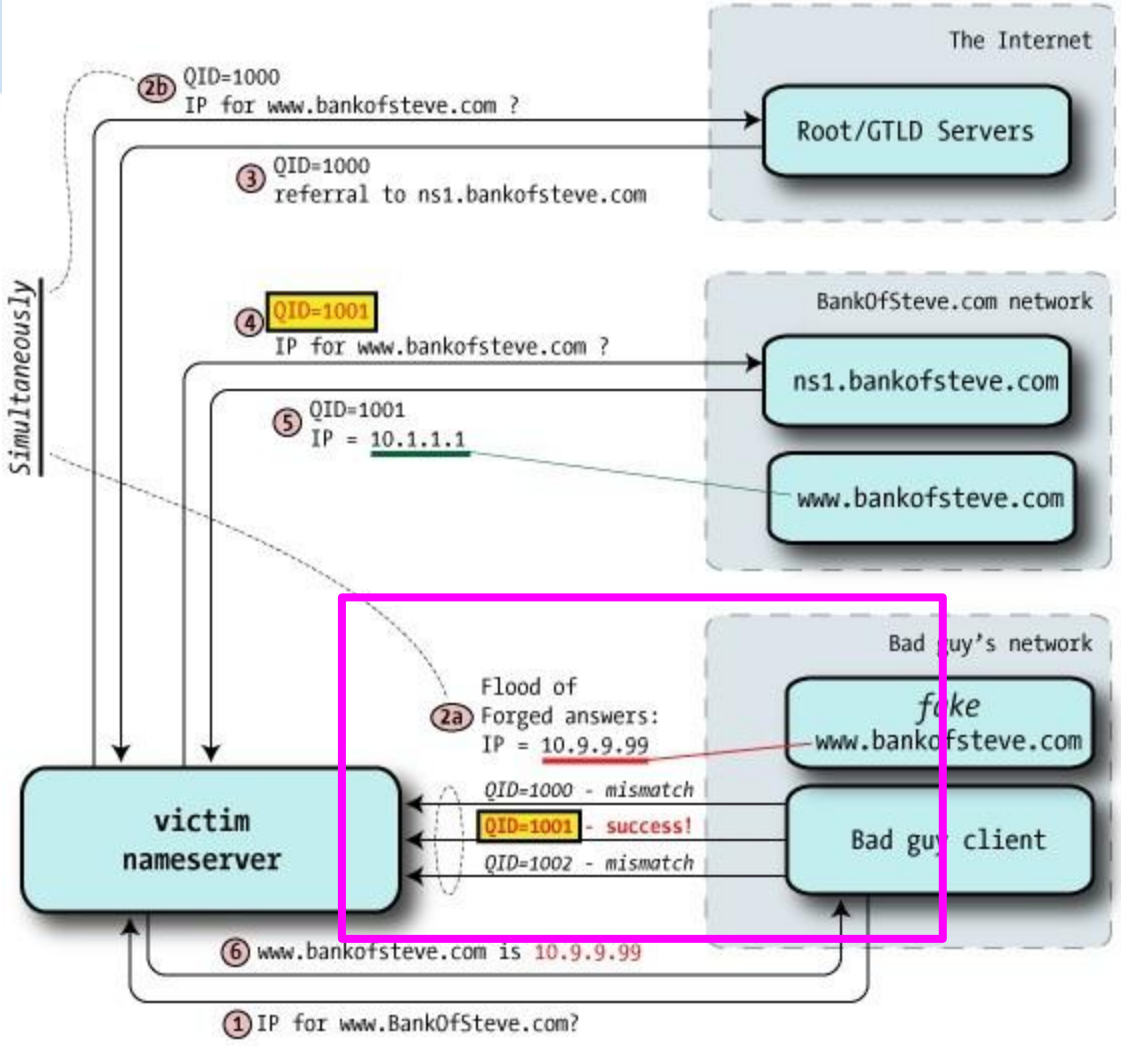
# Race with the real NS




Step 1 — Bad guy sends a DNS query to the victim nameserver for the hostname it wishes to hijack. This example assumes that the victim nameserver allows recursive queries from the outside world.

Step 2a — Knowing that the victim will shortly be asking ns1.bankofsteve.com (as directed from the root/GTLD servers) for an IP address, the bad guy starts flooding the victim with forged DNS reply packets. All purport to be from ns1.bankofsteve.com, but include the answer with the IP of badguy's fraudulent webserver.

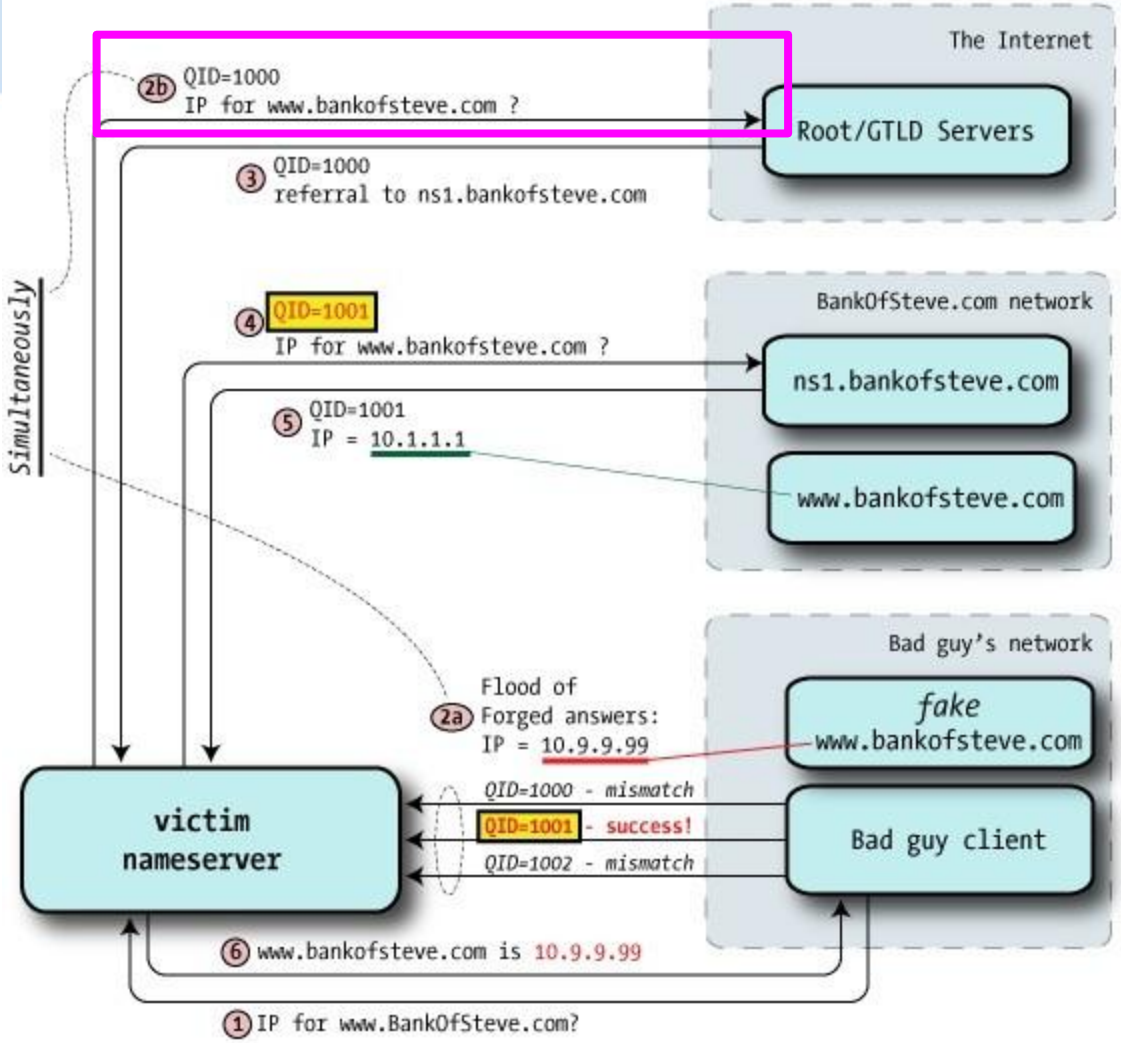
# Race with the real NS




Step 1 — Bad guy sends a DNS query to the victim nameserver for the hostname it wishes to hijack. This example assumes that the victim nameserver allows recursive queries from the outside world.

Step 2a — Knowing that the victim will shortly be asking ns1.bankofsteve.com (as directed from the root/GTLD servers) for an IP address, the bad guy starts flooding the victim with forged DNS reply packets. All purport to be from ns1.bankofsteve.com, but include the answer with the IP of badguy's fraudulent webserver.

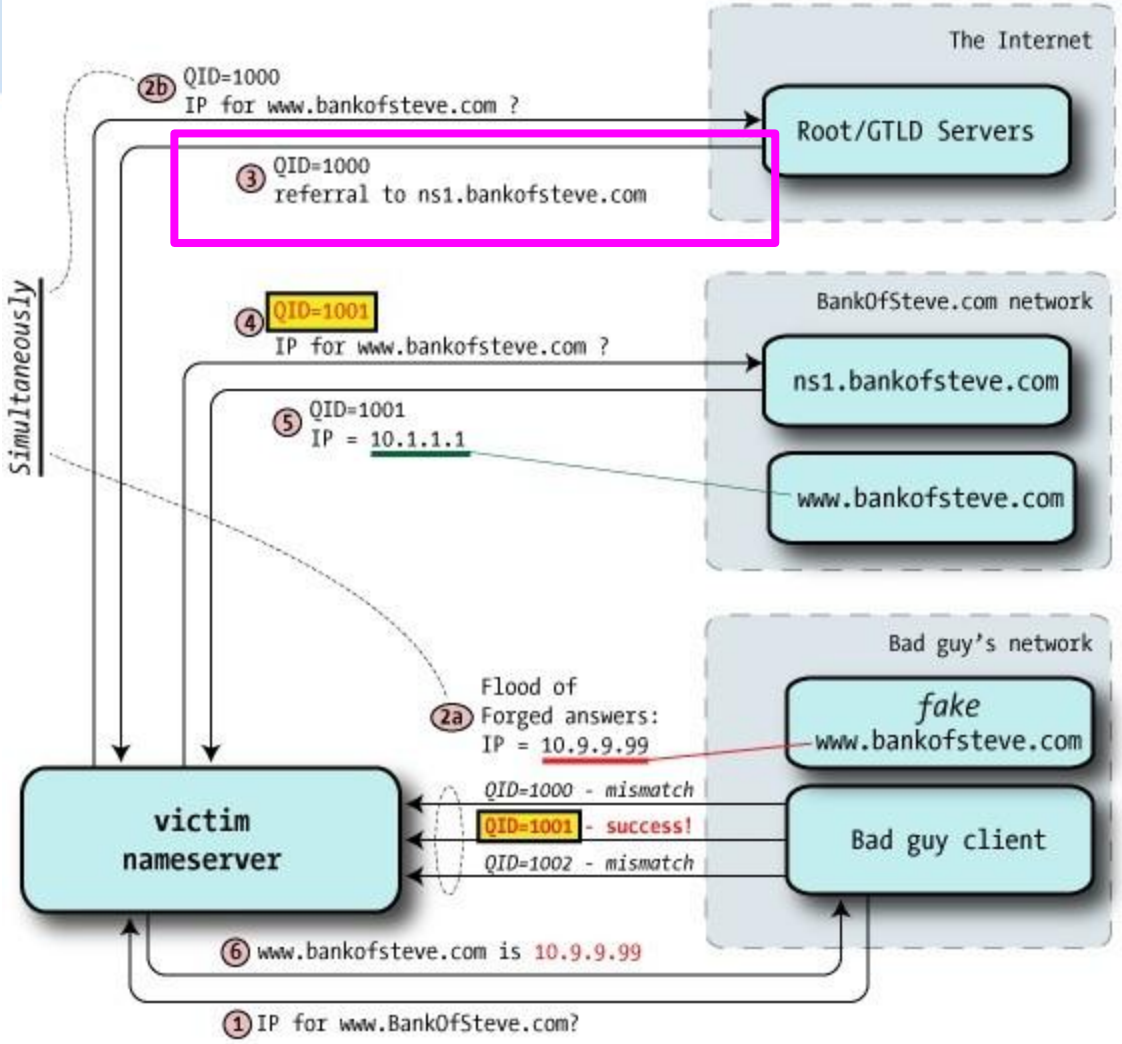
# Race with the real NS




Step 2a — Knowing that the victim will shortly be asking ns1.bankofsteve.com (as directed from the root/GTLD servers) for an IP address, the bad guy starts flooding the victim with forged DNS reply packets. All purport to be from ns1.bankofsteve.com, but include the answer with the IP of badguy's fraudulent webserver.

Steb 2b - The victim server is asking ns1.bankofsteve.com (as directed from the root/GTLD servers) for an IP address,

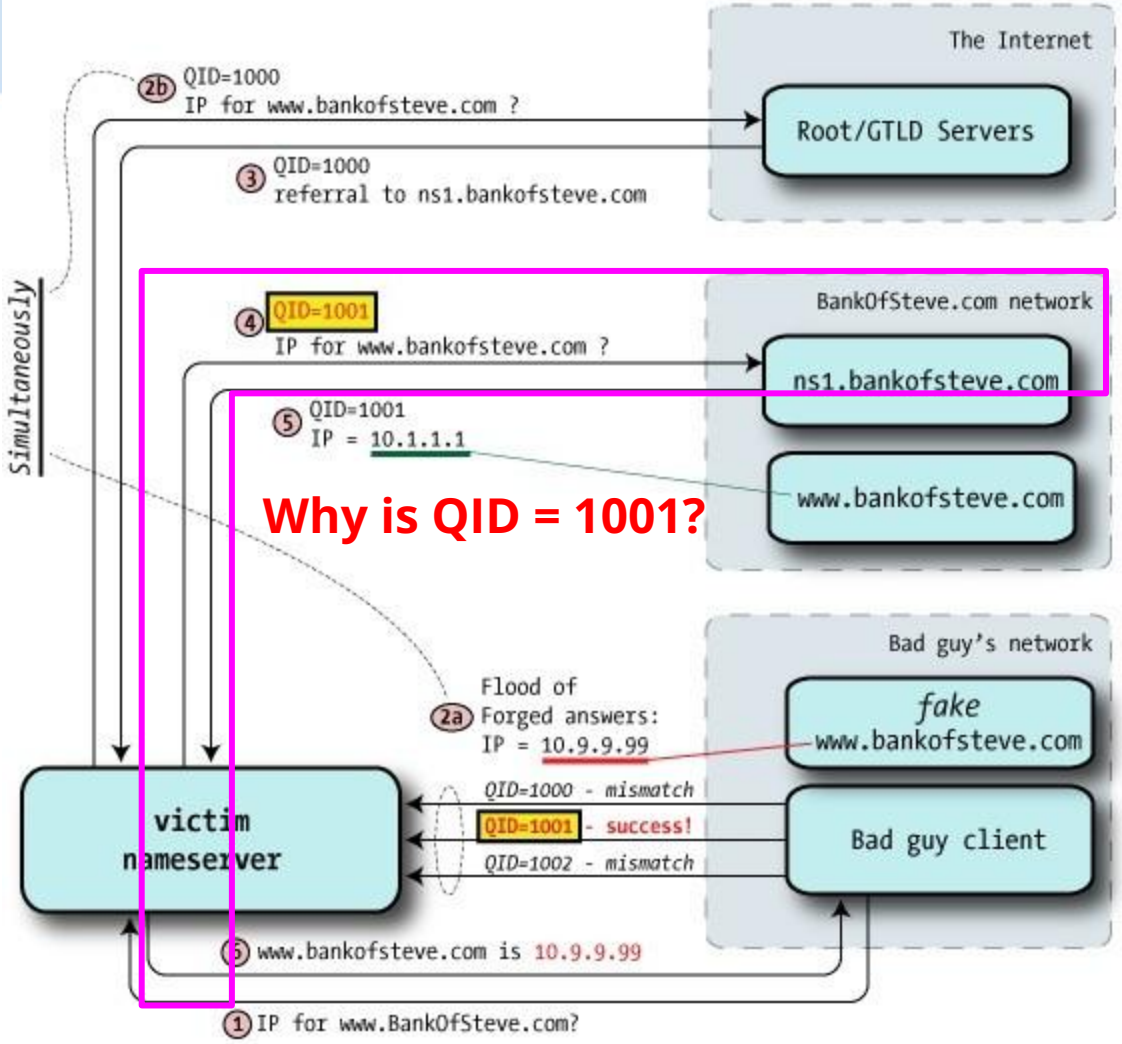
# Race with the real NS




- **Steps 2b & 3** — Root/GTLD servers provide referral to **ns1.bankofsteve.com**. This may be multiple queries, but we're showing just one for simplicity.

- **Step 4** — victim nameserver asks **ns1.bankofsteve.com** for the IP address of **www.bankofsteve.com**, and it uses query ID 1001 (one higher than the previous query).

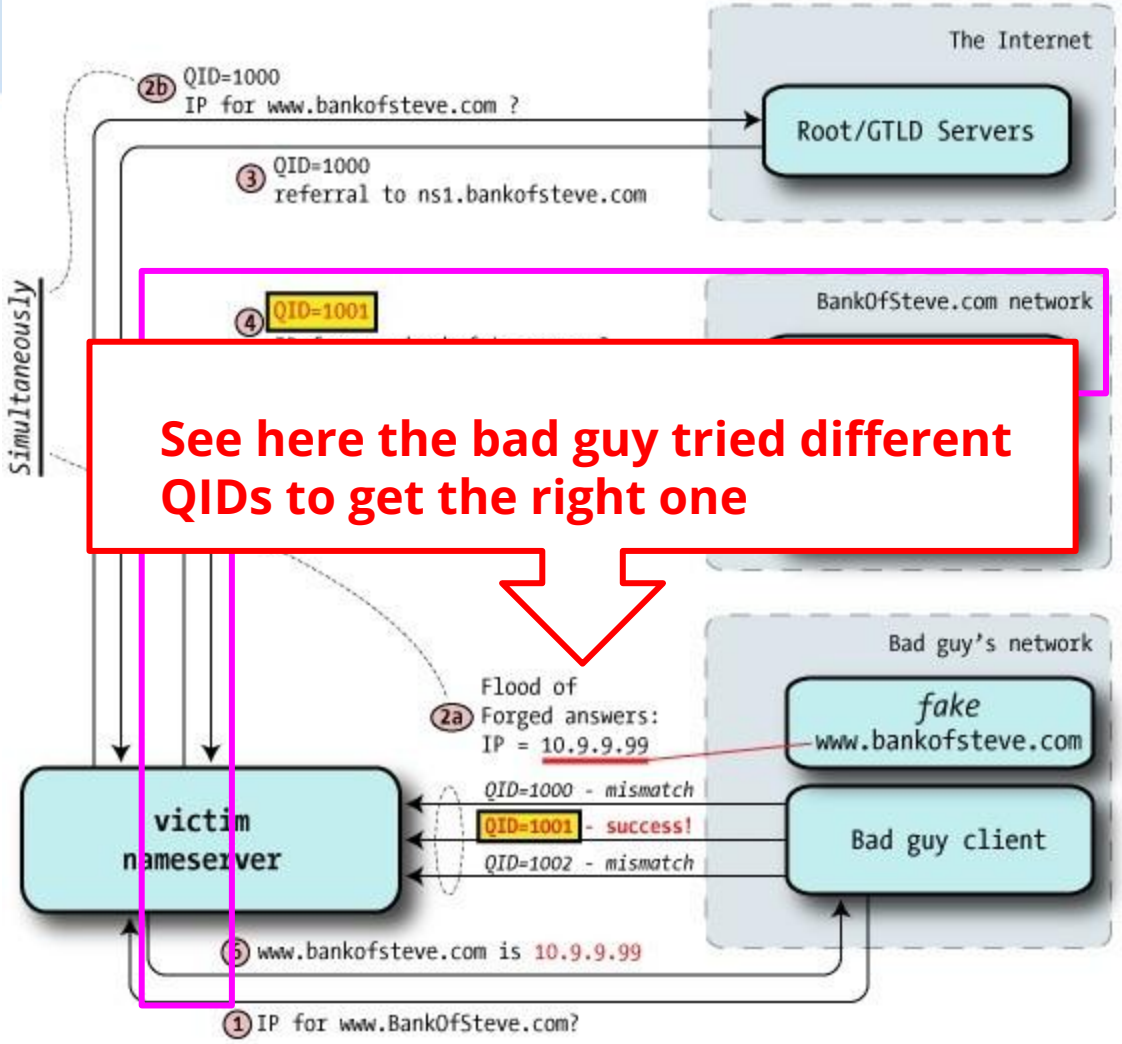
# Race with the real NS




- **Steps 2b & 3** — Root/GTLD servers provide referral to **ns1.bankofsteve.com**. This may be multiple queries, but we're showing just one for simplicity.

- **Step 4** — victim nameserver asks **ns1.bankofsteve.com** for the IP address of **www.bankofsteve.com**, and it uses query ID 1001 (one higher than the previous query).

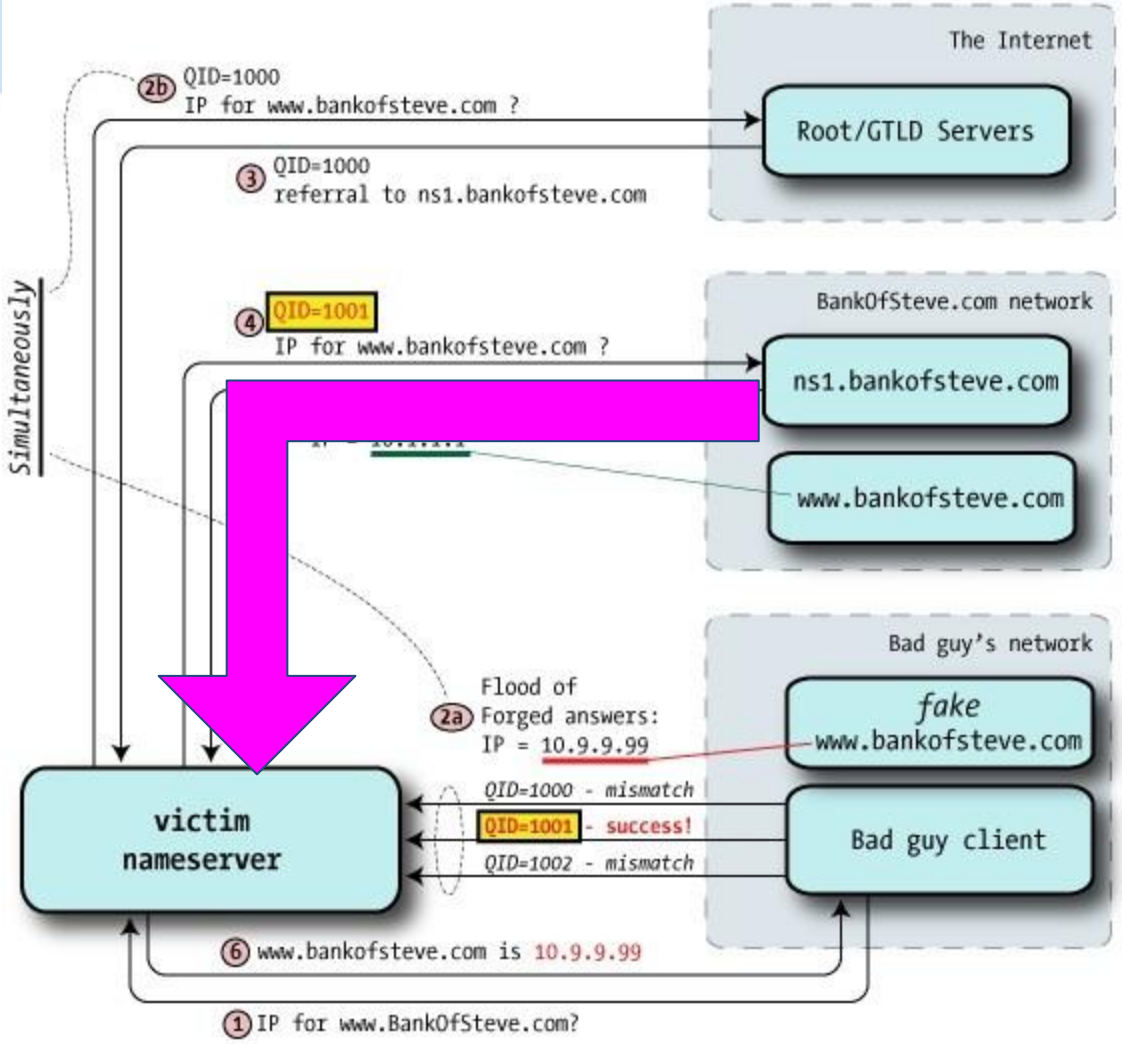
# Race with the real NS




- **Steps 2b & 3** — Root/GTLD servers provide referral to **ns1.bankofsteve.com**. This may be multiple queries, but we're showing just one for simplicity.

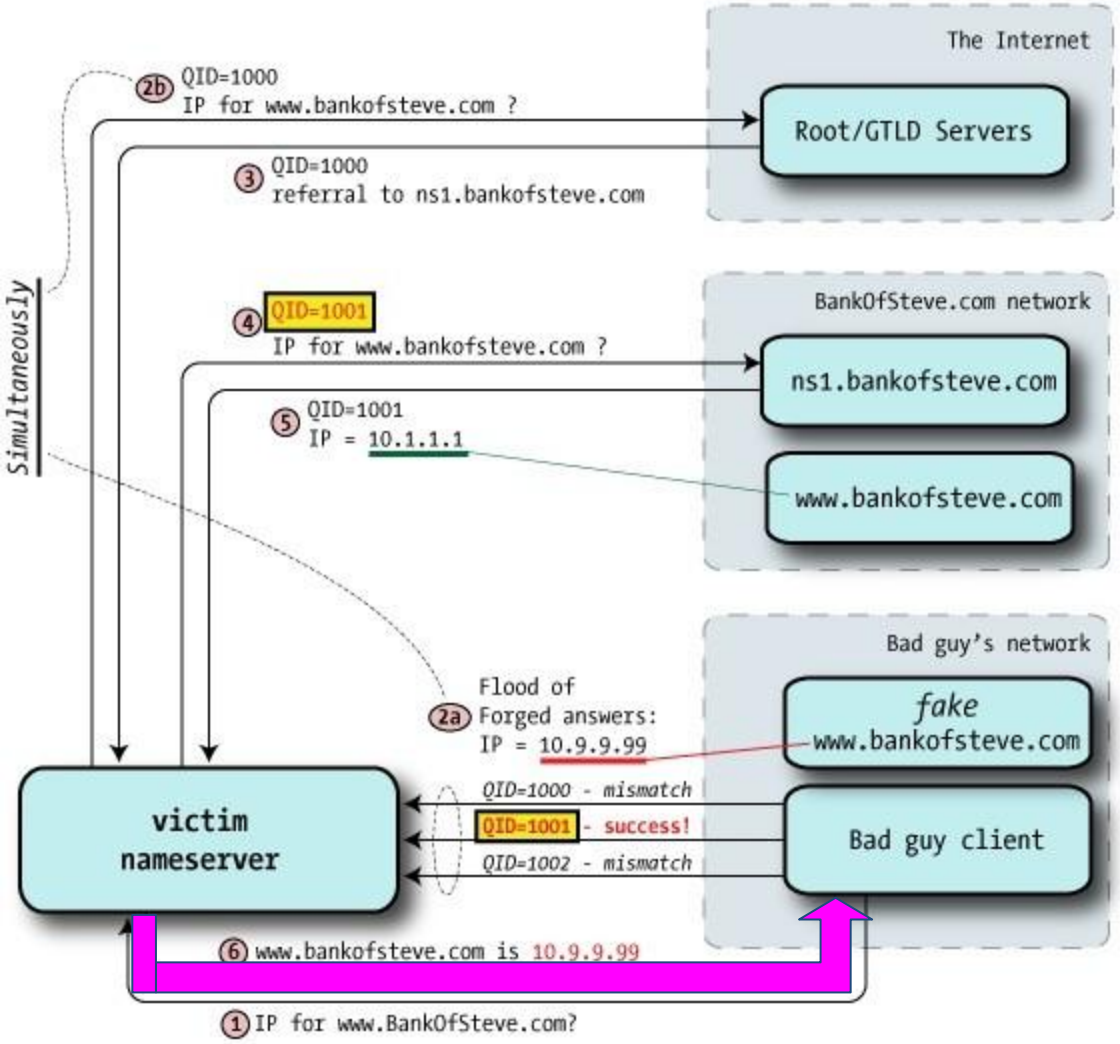
- **Step 4** — victim nameserver asks **ns1.bankofsteve.com** for the IP address of **www.bankofsteve.com**, and it uses query ID 1001 (one higher than the previous query).

# Race with the real NS

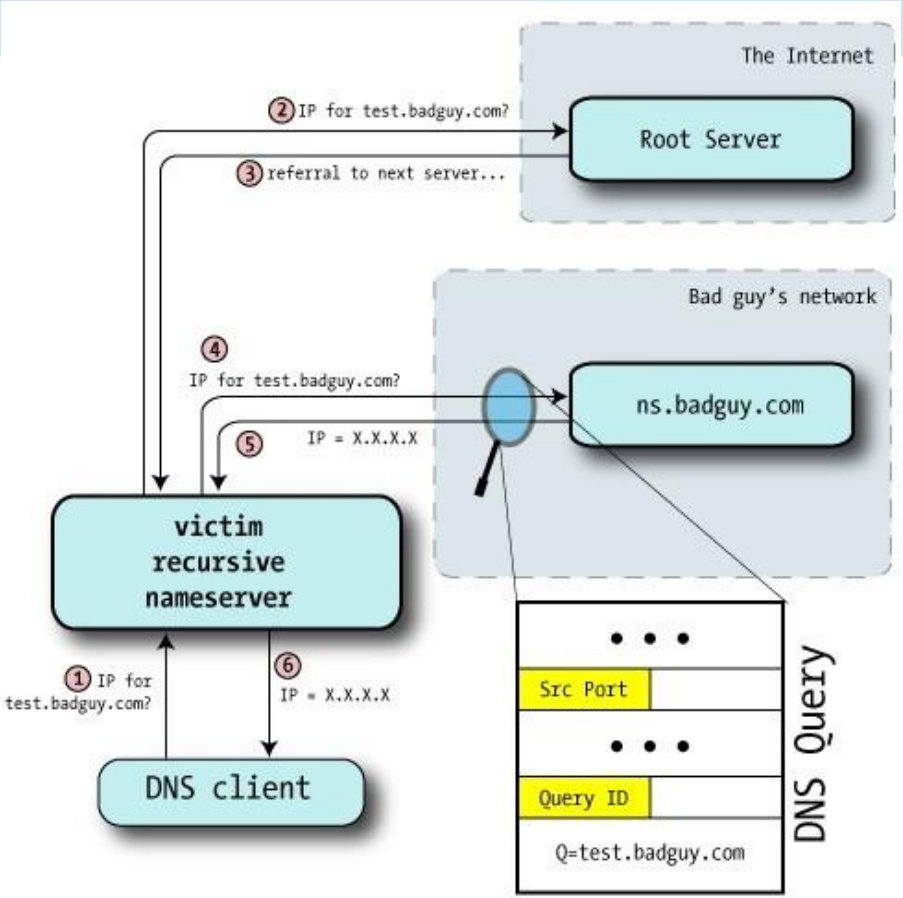



- **Step 5** — the real nameserver provides a legitimate response to this query, with QID=1001. But if the bad guy has successfully matched the query ID in the step **2a** flood, this legal reply arrives too late and is ignored. Oops.
- **Step 6** — With the bogus IP address (of the bad guy's webserver) in cache it provides this poisoned answer to the requesting DNS client. **Boom**.

# Race with the real NS




- **Step 5** — the real nameserver provides a legitimate response to this query, with QID=1001. But if the bad guy has successfully matched the query ID in the step **2a** flood, this legal reply arrives too late and is ignored. Oops.
- **Step 6** — With the bogus IP address (of the bad guy's webserver) in cache it provides this poisoned answer to the requesting DNS client. **Boom**.



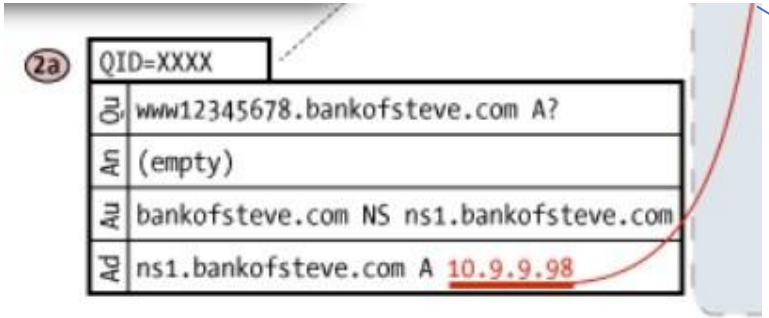

# How to predict the query ID and source port?

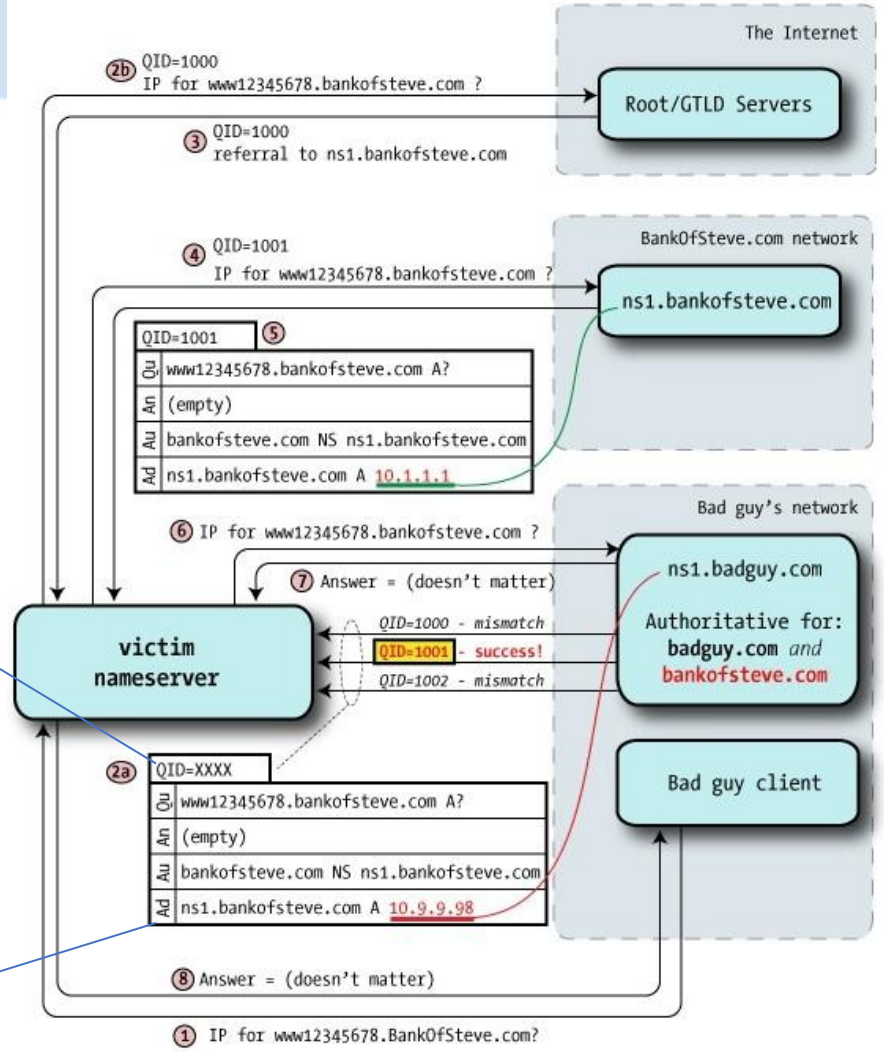
Another idea (Dan Kaminsky's attack):

- 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



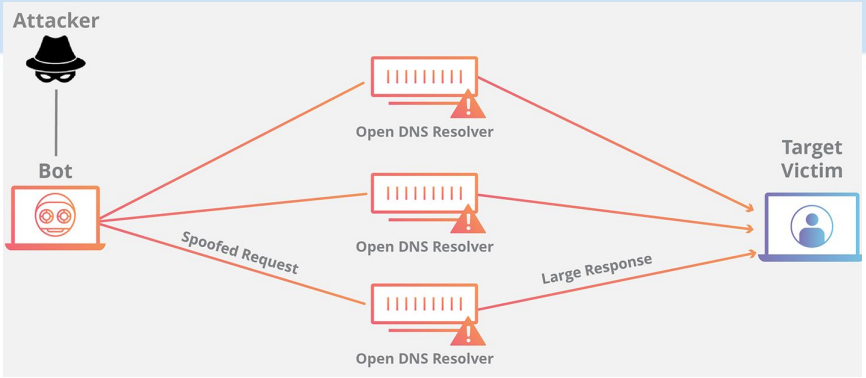



# Defenses (and attacks)

- 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

Share

## 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.

# Does happen in the wild

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

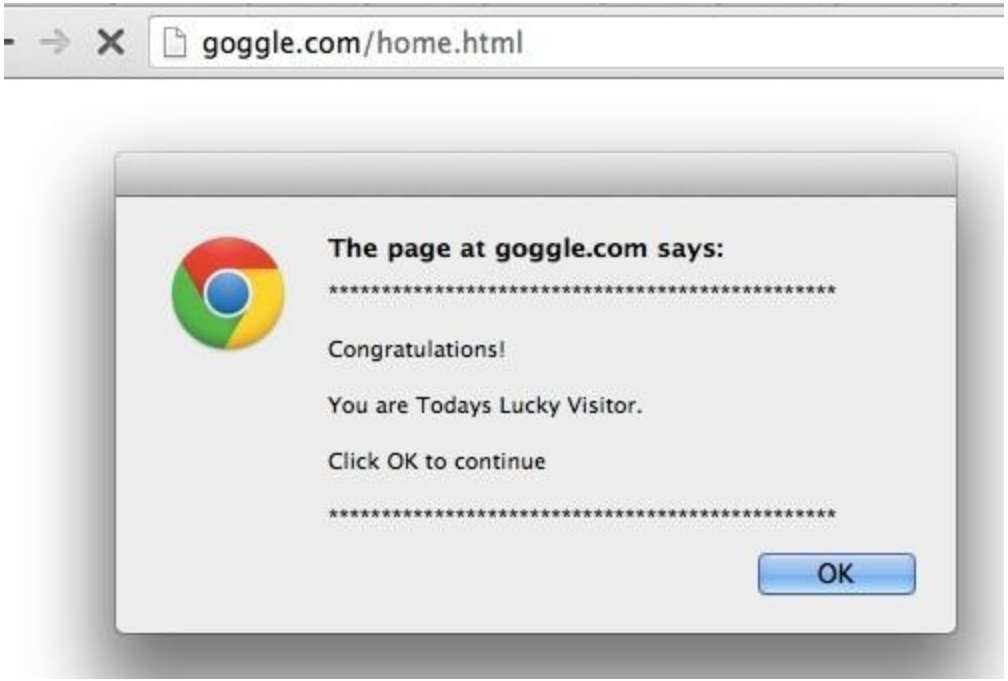
By Dancho Danchev | July 30, 2008, 8:08am PDT

***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

# 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

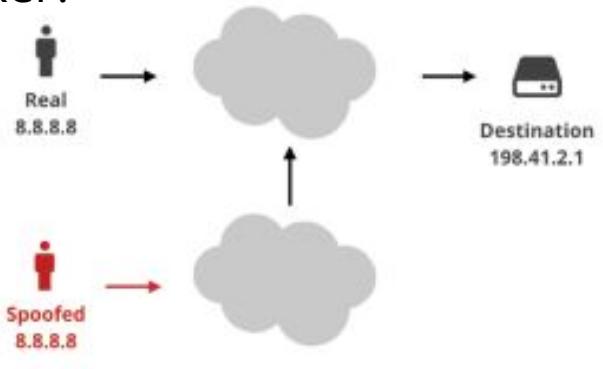

goggle.com/home.html
The page at goggle.com says:
**********
Congratulations!
You are Todays Lucky Visitor.
Click OK to continue
**********
OK


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!

# Network layer threats

**Spoofing:** Set arbitrary source address.

- IP packets offer no authentication.
- Source address in IP set by sender.
- Do you need to be a MITM/in-path attacker?



# Network layer threats

**Spoofing:** Set arbitrary source address.

- IP packets offer no authentication.
- Source address in IP set by sender.
- Do you need to be a MITM/in-path attacker?

  No! Off-path attacker can spoof a source address, but may not be able to see response sent to that address. When is this useful?

# Example: DHCP response spoofing

- DHCP = Dynamic Host Configuration Protocol
- used to configure hosts on network.
- DHCP is a protocol for *internal* networks and does not assign public IP addresses but private ones.

# Example: DHCP response spoofing

- Recall: DHCP used to configure hosts on network.
- DHCP requests broadcast to local network.
- Local attacker can race real server for response, set victim's network gateway and DNS server to attacker-controlled values.
- Allows attacker to act as invisible man-in-the-middle and relay victim's traffic.

# Network layer threats

**Set arbitrary destination address:**
No authentication of traffic sender at network layer

Applications:

- **Network scanning:**
  - Example tools: nmap, zmap, shodan
  - IPv4 has $2^{32}$ possible addresses, possible to enumerate all of them.
  - Send traffic to a port on some protocol, if you get a response then there is a live service.
- **Unwanted traffic:**
  - Denial of service attacks: overwhelm recipient with traffic

TECH | FACEBOOK | INSTAGRAM

# Facebook is back online after a massive outage that also took down Instagram, WhatsApp, Messenger, and Oculus

81

*'Networking issues' took the sites down just before noon ET*

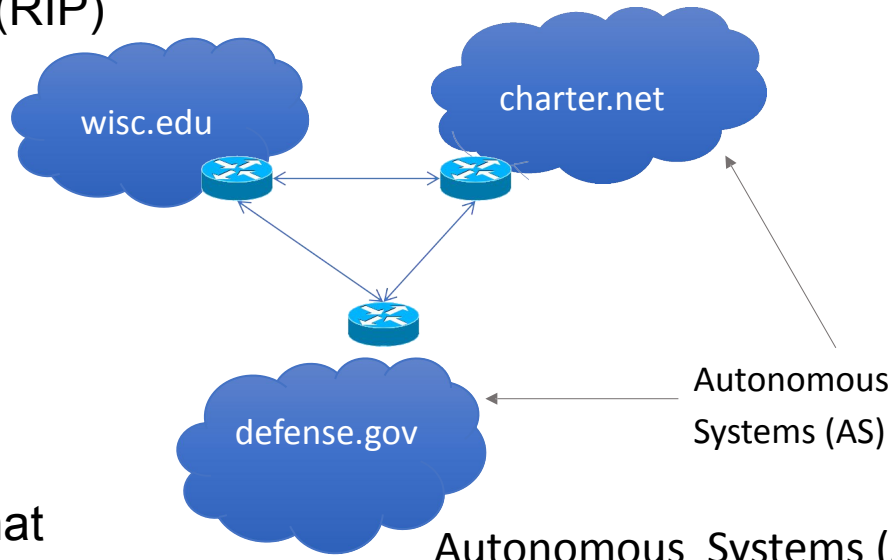
By Richard Lawler and Alex Heath | Updated Oct 5, 2021, 2:28pm EDT

# 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 - Border Gateway Protocol

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

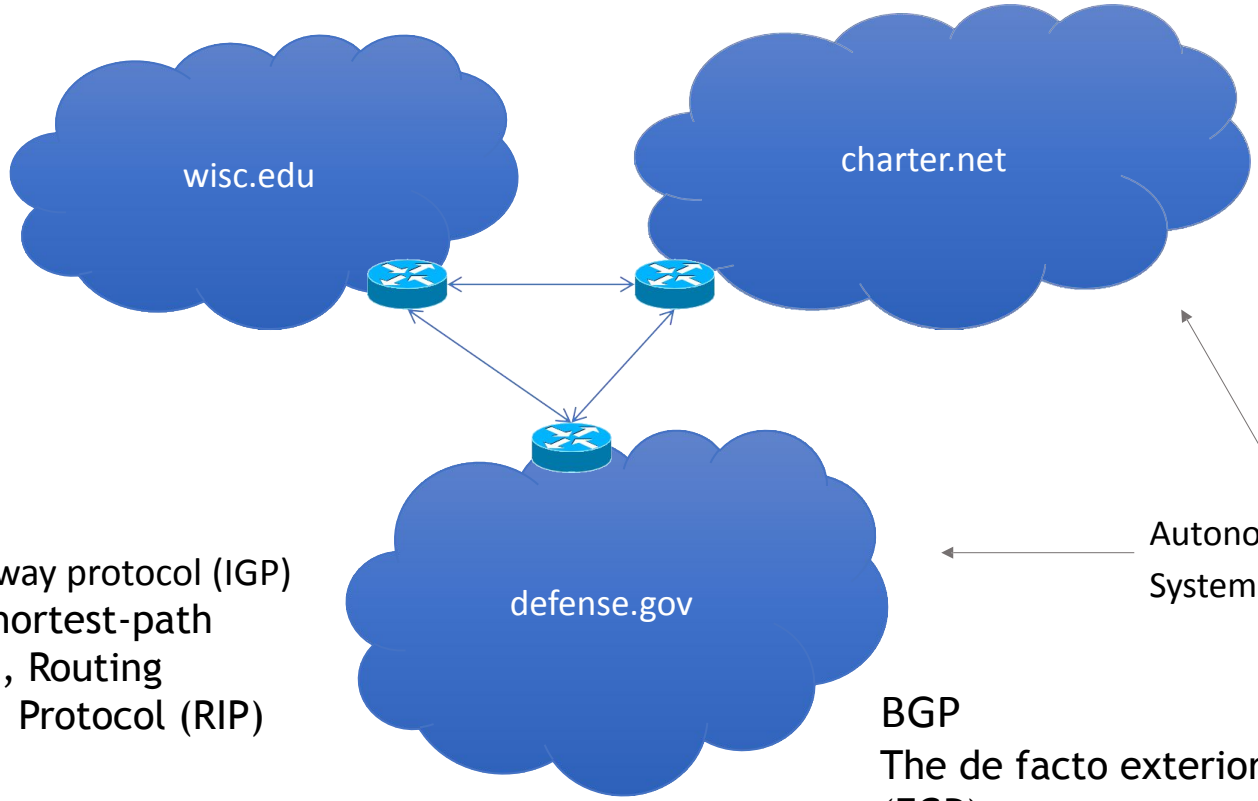



BGP

- The de facto exterior gateway protocol (EGP)
- Inter-AS routing protocol that helps AS get info from other AS, send info to routers in the AS and determine routes to subnets

Autonomous Systems (AS) - group of routers that are typically operated by the same ISP, company, etc.

# BGP and routing

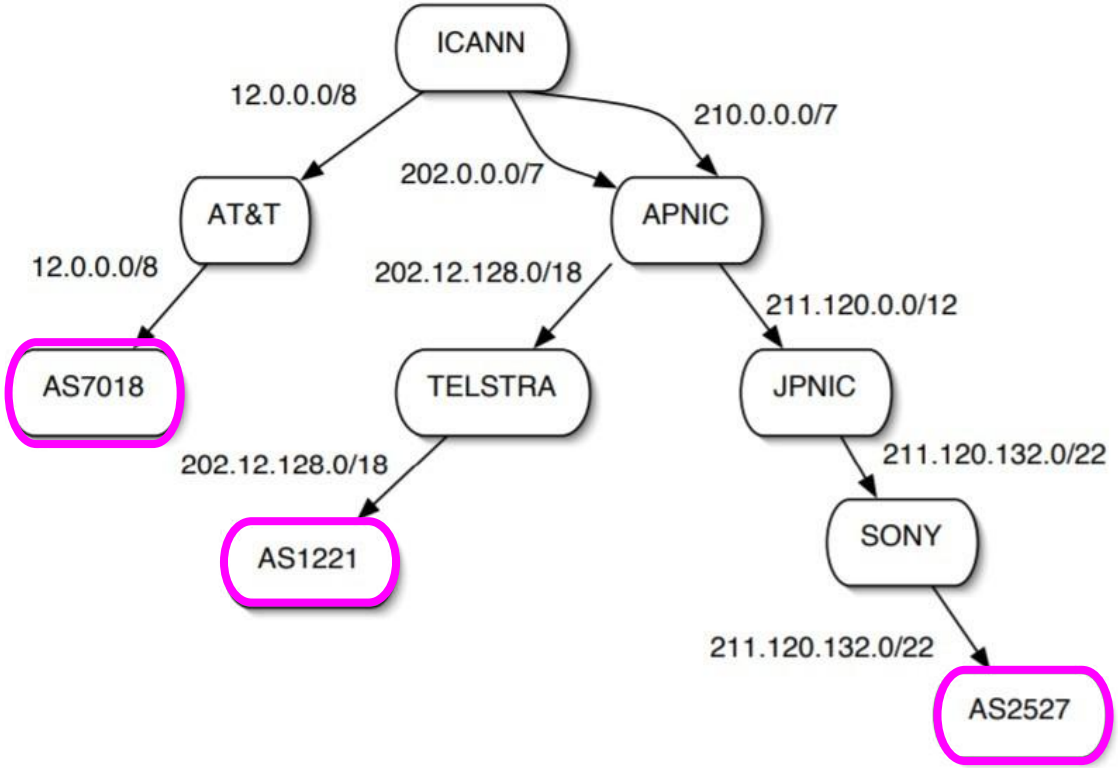



Interior Gateway protocol (IGP)
E.g, Open shortest-path first (OSPF), Routing Information Protocol (RIP)

BGP
The de facto exterior gateway protocol (EGP)

A sample address delegation graph for a small part of the IPv4 address space. The address space is administered by ICANN, and hence all delegation flows from that organization

ASes are assigned an AS number (ASN) in a similar manner, with ICANN being the ultimate authority for delegating numbers.

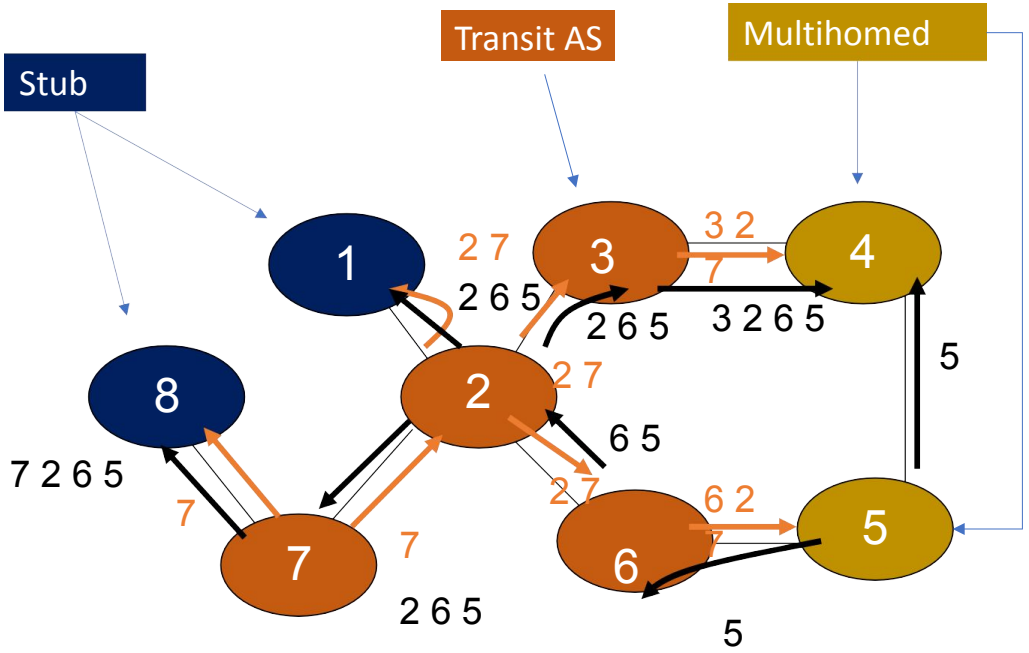



Source:
http://patrickmcdaniel.org/pubs/td-5ugj33.pdf

# 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
- Hijacking
  - prefix hijacking
  - route hijacking
  - border gateway protocol (BGP) hijacking

# Network layer threats

**Misdirection:** BGP hijacking.

- Recall: BGP protocol manages IP routing information between networks on the internet.
- Each BGP node maintains connections to a set of trusted neighbors.
- Neighbors share routing information.
- Routes are not authenticated: malicious or malfunctioning nodes may provide incorrect routing information that redirects IP traffic.

# 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


https://www.noction.com/blog/bgp-security-prefixes-authorization

**GOVERNMENT OF PAKISTAN**
**PAKISTAN TELECOMMUNICATION AUTHORITY**
**ZONAL OFFICE PESHAWAR**

Plot-11, Sector A-3, Phase-V, Hayatabad, Peshawar.
Ph: 091-9217279- 5829177 Fax: 091-9217254
www.pta.gov.pk

NWFP-33-16 (BW)/06/PTA February ,2008

Subject: **Blocking of Offensive Website**

*Reference:* *This office letter of even number dated 22.02.2008.*

I am directed to request all ISPs to immediately block access to the following website

URL: http://www.youtube.com/watch?v=o3s8jtvvg00

IPs: 208.65.153.238, 208.65.153.253, 208.65.153.251

Compliance report should reach this office through return fax or at email peshawar@pta.gov.pk today please.

**Deputy Director**
(Enforcement)

To:
1. M/s Comsats, Peshawar.
2. M/s GOL Internet Services, Peshawar.
3. M/s Cyber Internet, Peshawar.
4. M/s Cybersoft Technologies, Islamabad.

# 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…

Apr 24, 2018, 02:10pm EDT

# A $152,000 Cryptocurrency Theft Just Exploited A Huge 'Blind Spot' In Internet Security

**Thomas Brewster** Forbes Staff

Cybersecurity

*Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.*

Follow


Welcome Andree

HOME | AUTONOMOUS SYSTEMS | PREFIXES | ALERTS | PEERMON

## My Alerts

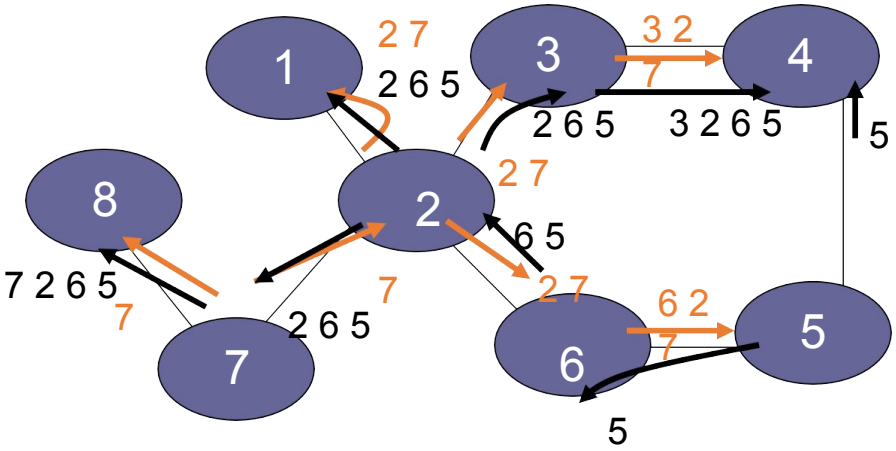
### Alerts Details

Tools

**On Saturday March 15th 2014 at 17:23 UTC we detected a Origin AS Change event for your prefix (8.8.8.0/24 *Google DNS*)**
**The detected prefix: 8.8.8.8/32, was announced by AS7908 (BT LATAM Venezuela, S.A.)**

| | |
|---|---|
| Alert description: | Origin AS Change |
| Detected Prefix: | 8.8.8.0/24 |
| Detected Origin AS: | 7908 |
| Expected Origin AS: | 15169 |

# BGPsec




- 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)



## BGPSec – A reality now

[RFC 8205]

Need to wait for ASes to catch up!

# TCP threats

Recall:

- TCP session identified by (source address, source port, destination address, destination port)
- TCP packets identified by sequence number that determines where in stream they are placed.

**On-path injection**

- Connection hijacking: If an on-path attacker knows ports and sequence numbers, can inject data into the TCP connection.
- RST injection: Attacker can inject RST into connection to immediately stop it, will be accepted if sequence number is within acceptable window.

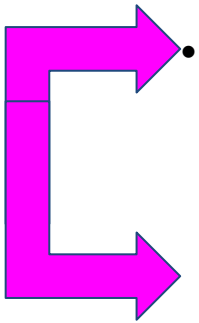
# TCP threats

Recall:

- TCP session identified by (source address, source port, destination address, destination port)
- TCP packets identified by sequence number that determines where in stream they are placed.

**On-path injection**

- Connection hijacking: If an on-path attacker knows ports and sequence numbers, can inject data into the TCP connection.
- RST injection: Attacker can inject RST into connection to immediately stop it, will be accepted if sequence number is within acceptable window.



Reset TCP Packet which is used to notify the packet the receiver that the sender will no longer accept incoming packets

# Great Firewall of China

- China does extensive monitoring of all cross-border network traffic and blocks many international services and sites
- Collection of network techniques and policies called the “Great Firewall”
- Most famously: RST injection based on IP/host blocking and deep packet inspection for blacklisted keywords
- Multi-decade arms race on censorship circumvention
- Circumvention techniques: HTTPS, VPNs, proxies, traffic obfuscation, domain fronting, refraction networking

GREATFIRE.ORG

SEARCH TEST URL TEST KEYWORD FAQ NEWS

# WE ARE UNDER ATTACK

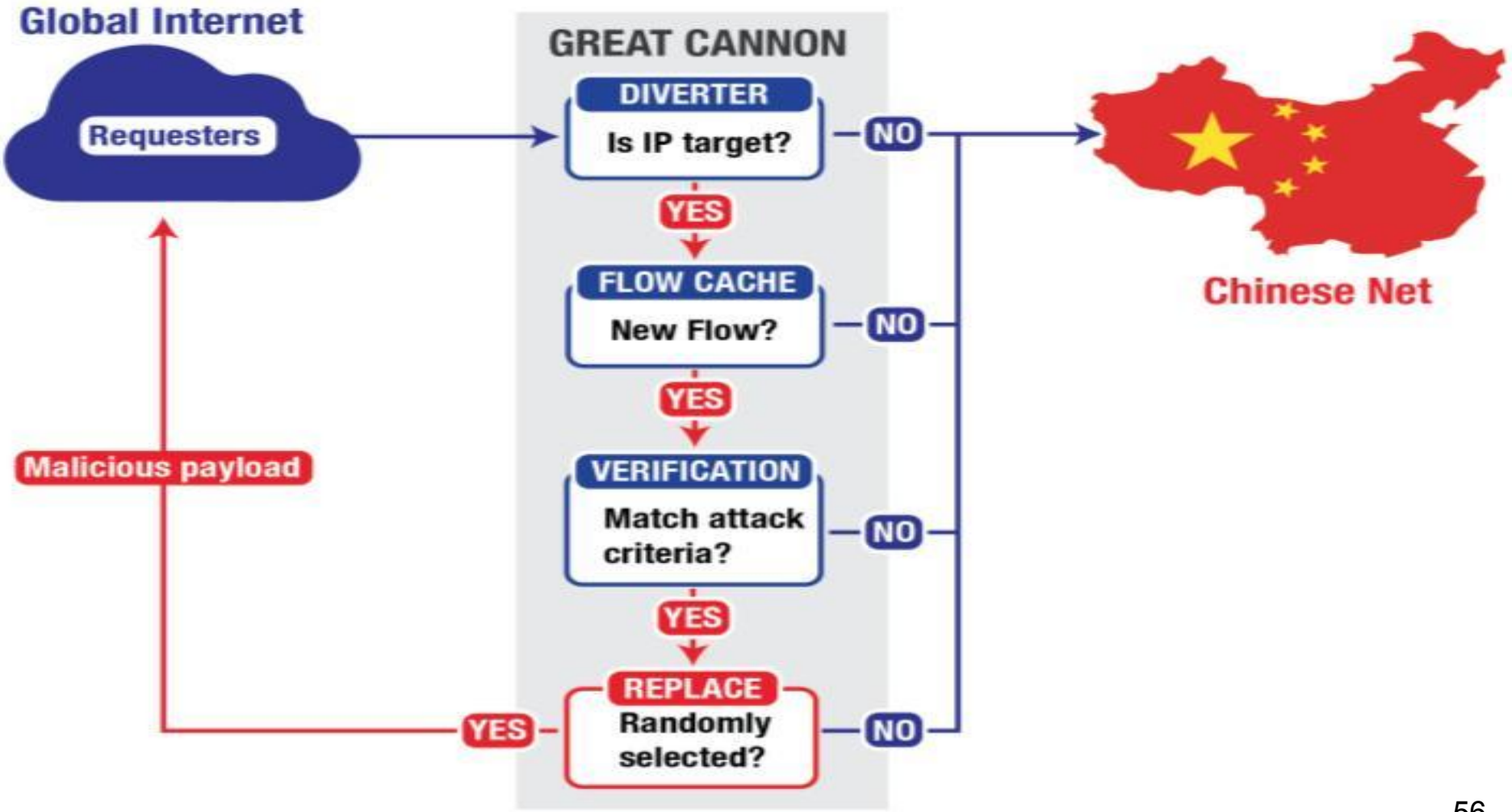
Submitted by charlie on Thu, Mar 19, 2015

We are under attack and we need help.

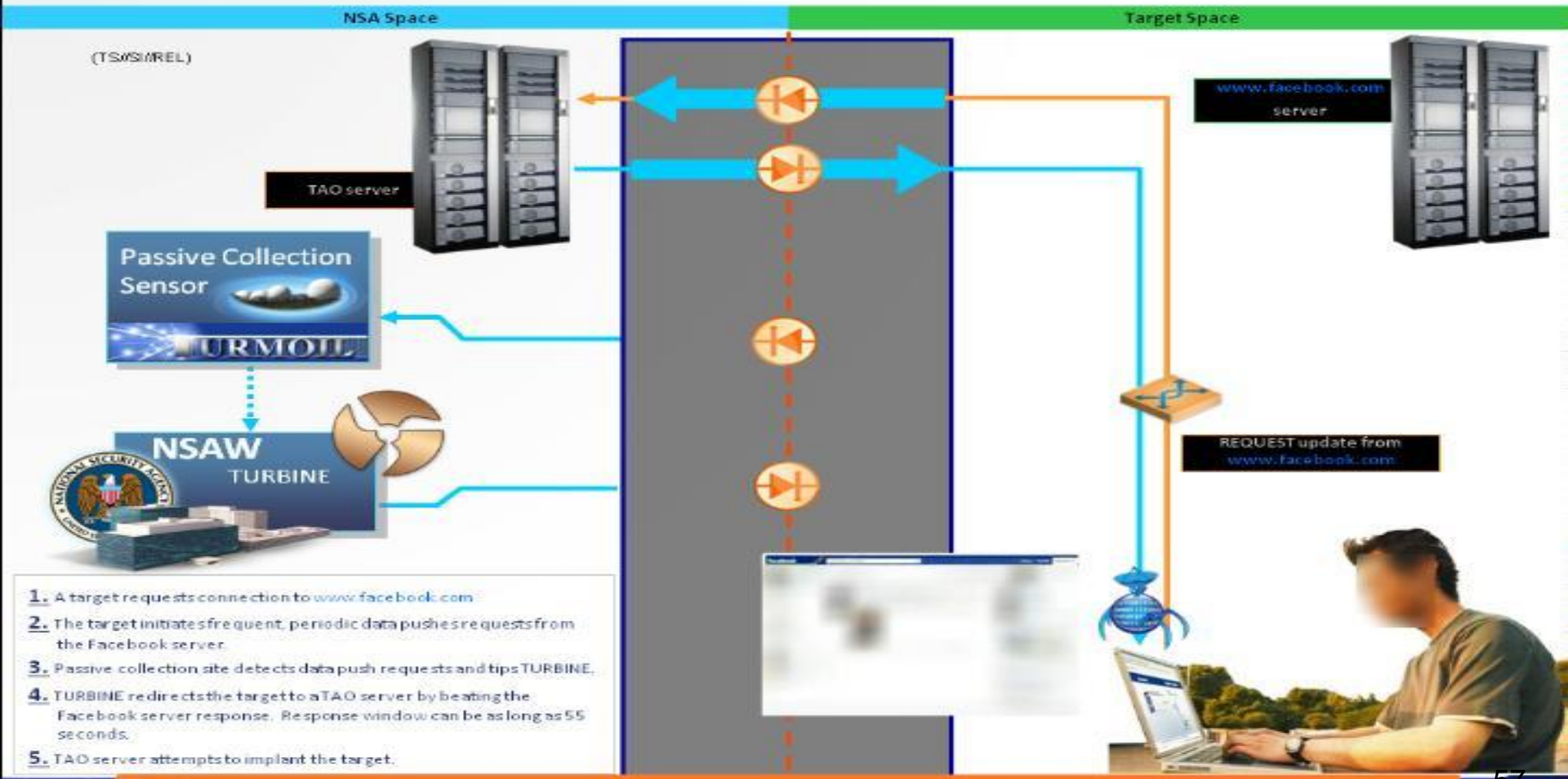
Likely in response to a recent story in the Wall Street Journal (WSJ), we've experienced our first ever distributed denial of service (DDoS) attack. This tactic is used to bring down web pages by flooding them with lots of requests – at the time of writing they number 2.6 billion requests per hour. Websites are not equipped to handle that kind of volume so they usually "break" and go offline.

This kind of attack is aggressive and is an exhibition of censorship by brute force. Attackers resort to tactics like this when they are left with no other options.

We are not equipped to handle a DDoS attack of this magnitude and we need help. Some background:


Global Internet
Requesters
GREAT CANNON
DIVERTER
Is IP target?
NO
YES
FLOW CACHE
New Flow?
NO
YES
VERIFICATION
Match attack criteria?
NO
YES
REPLACE
Randomly selected?
NO
YES
Malicious payload
Chinese Net

# (TS//SI//REL) QUANTUMHAND



# TCP threats

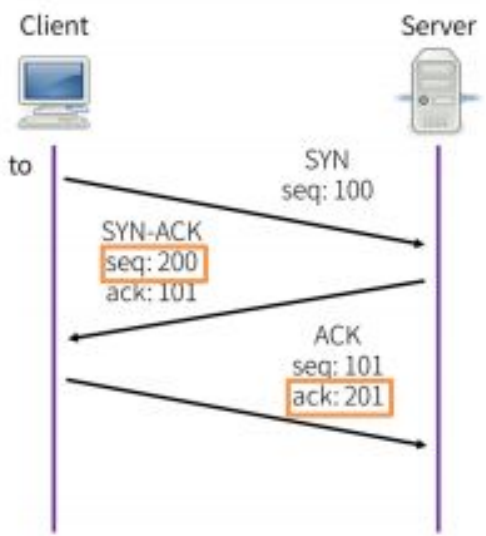
**Blind spoofing**: Can an off-path attacker convince a victim to open a TCP connection with a spoofed host?

- Attacker forges the initial TCP handshake SYN message from an arbitrary source.
- The attacker cannot see the SYN-ACK response so does not learn the responder's sequence number.

# TCP threats

**Blind spoofing**: Can an off-path attacker convince a victim to open a TCP connection with a spoofed host?

• Attacker forges the initial TCP handshake SYN message from an arbitrary source.
• The attacker cannot see the SYN-ACK response so does not learn the responder's sequence number.
• Initial TCP spec: initial sequence number based on local clock: easy to brute force
• Mitigation: use random ISN: 2 −32 chance of guessing correctly.



# Physical/link layer threats

**Eavesdropping:** Violates confidentiality.

Who can see the packets you send?

- Network (routers, switches, access points) see all traffic passing by.

# Physical/link layer threats

**Eavesdropping:** Violates confidentiality.

Who can see the packets you send?

- Network (routers, switches, access points) see all traffic passing by.

- Unprotected WiFi network:
- WPA2 Personal (PSK):
- Non-switched Ethernet:
- Switched Ethernet:

# Network eavesdropping

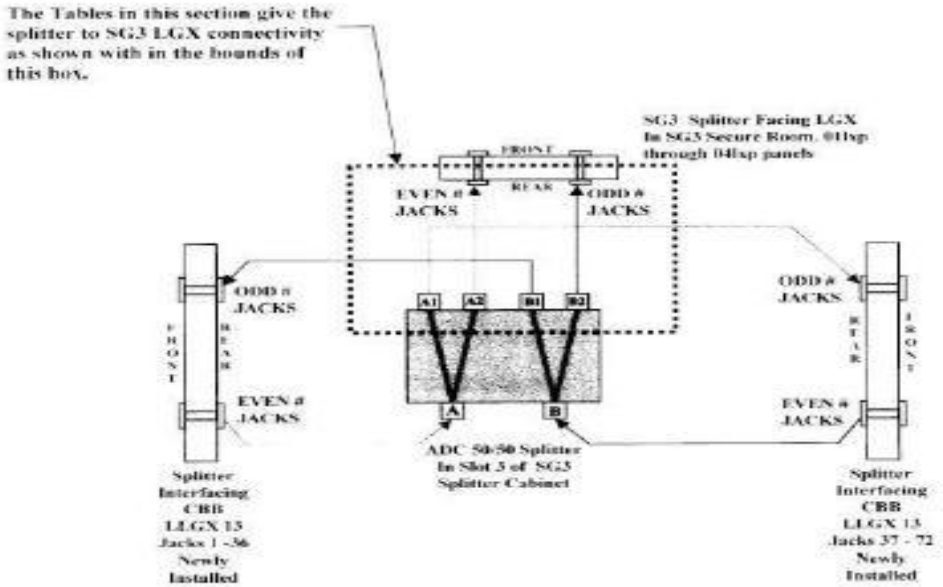
## Tools like tcpdump and Wireshark let you capture local network traffic

```
$ sudo tcpdump -v -n - i eno1
tcpdump: l i st e n i n g on eno1, link-type EN10MB (Ethernet), capture size 262144 bytes
17:29:41.757880 IP (tos 0x10, t t l 64, id 38565, o f f se t 0 , f l a g s [DF], proto TCP( 6 ) , length 176)14) 132.239.15.243.4258 > 66.10.100.54.62681:
Flags [ P . ] , cksum 0x3bc5 (incorrect -> 0x2e82), seq 1687079
17:29:41.770734 IP (tos 0x0, ttl 50, id 0 , o f f se t 0 , f l a g s [DF], proto TCP ( 6 ) , length 52) 66.10.100.54.62681 > 132.239.15.243.4258: Flags [ . ] ,
cksum 0x8e71 ( c o r r e c t ) , ack 124, win 11736, opti
17:29:41.789239 ARP, Ethernet (len 6 ) , IPv4 (len 4 ) , Request who-has 132.239.15.119 t e l l 132.239.15.1, l e
17:29:41.936864 IP (tos 0x0, ttl 1 , id 20121, o f f set 0 , f l ag s [none], proto UDP (17), length 202) 132.239.15.210.65021 > 239.255.255.250.1900: UDP,
length 174 17:29:42.036268 IP6 (hlim 1 , next-header UDP (17) payload length: 83) fe80::225:b3ff:fefa:a13d.546 > ff02
17:29:42.390349 IP (tos 0x0, ttl 64, id 35459, o f f se t 0 , f l a g s [DF], proto UDP (17), length 51) 132.239.15.243.40288 > 172.217.4.138.443: UDP,
length 23
17:29:42.419390 IP (tos 0x0, ttl 57, id 0 , o f f se t 0 , f l a g s [DF], proto UDP (17), length 48) 172.217.4.138.443 > 132.239.15.243.40288: UDP, length 20
17:29:42.443102 ARP, Ethernet (len 6 ) , IPv4 (len 4 ) , Request who-has 132.239.15.34 t e l l 132.239.15.1, len
17:29:42.541827 STP 802.1w, Rapid STP, Flags [Learn, Forward], bridge-id 81b0.00:a3:d1:25:06:00.801a, len message-age 2.00s, max-age 20.00s,
hello-time 2.00s, forwarding-delay 15.00s root-id 21b0.3c:08:f6:21:a8:40, root-pathcost 2001, port-role Designated
17:29:43.752250 IP (tos 0x0, ttl 64, id 61970, o f f se t 0 , f l a g s [DF], proto TCP ( 6 ) , length 109) 132.239.15.243.55866 > 52.37.243.173.443: Flags [ P .
] , cksum 0xbd14 (incorrect -> 0xcfbd), seq 3280138
17:29:43.788285 IP (tos 0x0, ttl 38, id 43082, o f f set 0 , f l ag s [DF], proto TCP ( 6 ) , length 109) 52.37.243.173.443 > 132.239.15.243.55866: Flags [ P . ]
, cksum 0x65eb ( c o r r e c t ) , seq 1:58, ack 57, win 8
17:29:43.788311 IP (tos 0x0, t t l 64, id 61971, o f f se t 0 , f l a g s [DF], proto TCP( 6 ) , length 52) 132.239.15.243.55866 > 52.37.243.173.443: Flags [ . ] ,
cksum 0xbcdb (incorrect -> 0xab20), ack 58, win
17:29:43.905367 IP (tos 0x0, ttl 128, id 19913, o f f se t 0 , f l a g s [none], proto UDP (17), length 414) 132.239.15.14.17500 > 255.255.255.255.17500:
UDP, length 386
17:29:43.907037 IP (tos 0x0, ttl 128, id 59034, o f f set 0 , f l ag s [none], proto UDP (17), length 414) 132.239.15.14.17500 > 132.239.15.255.17500:
UDP, length 386 17:29:43.907052 IP (tos 0x0, ttl 128, id 19914, o f f se t 0 , f l a g s [none], proto UDP (17), length 414) 132.239.15.14.17500 >
255.255.255.255.17500: UDP, length 386 17:29:43.907057 IP (tos 0x0, ttl 128, id 19915, o f f se t 0 , f l a g s [none], proto UDP (17), length 414)
132.239.15.14.17500>255.255.255.255.17500:UDP,length386
```

# Advanced threats: Physical cables can be tapped

Mathew F. Casamassima, (732) 420-2033, mcasamassima@att.com

# Splitter to SG3 LGX Connectivity



# (TS//SI//NF) FAA702 Operations

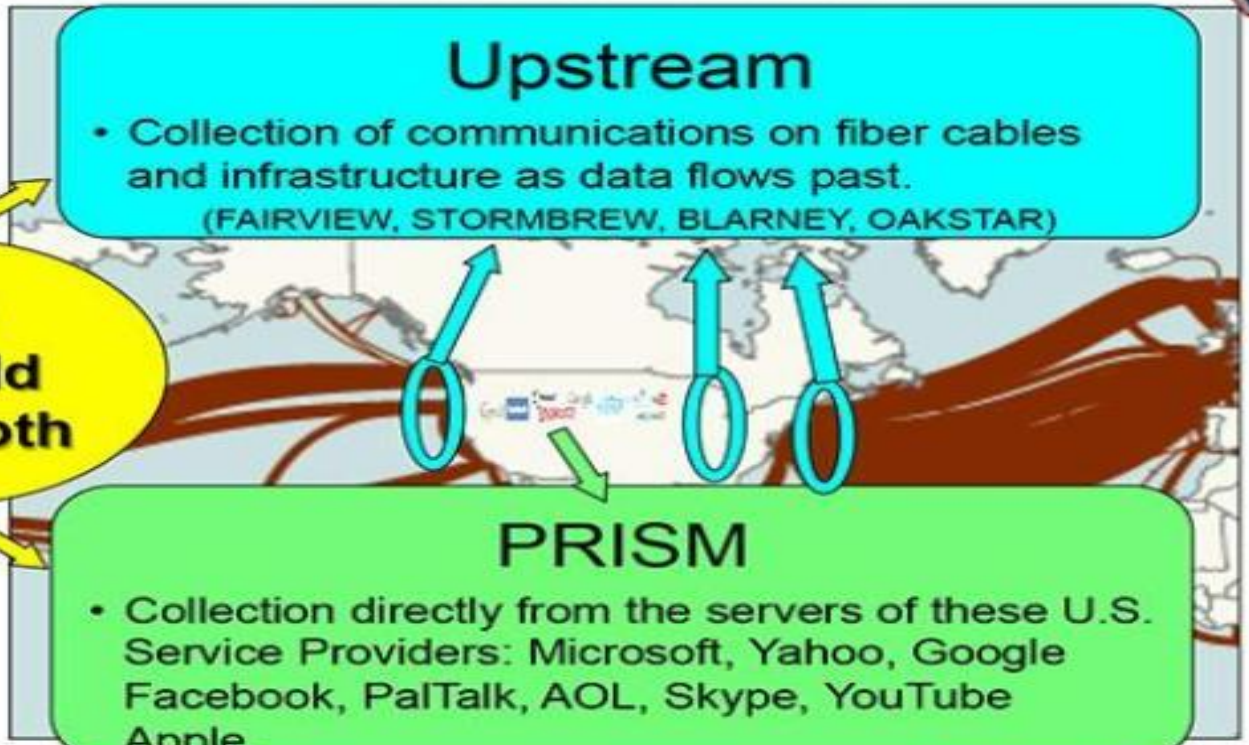
*Two Types of Collection*

## Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.

(FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

**You Should Use Both**



## PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

# Optic Nerve

"Optic Nerve was based on collecting information from GCHQ's huge network of internet cable taps, which was then processed and fed into systems provided by the NSA. Webcam information was fed into NSA's XKeyscore search tool, and NSA research was used to build the tool which identified Yahoo's webcam traffic."

– The Guardian 2/27/14

# Optic Nerve

"Optic Nerve was based on collecting information from GCHQ's huge network of internet cable taps, which was then processed and fed into systems provided by the NSA. Webcam information was fed into NSA's XKeyscore search tool, and NSA research was used to build the tool which identified Yahoo's webcam traffic." – The Guardian 2/27/14

27. Unfortunately, there are issues with undesirable images within the data. It would appear that a surprising number of people use webcam conversations to show intimate parts of their body to the other person. Also, the fact that the Yahoo software allows more than one person to view a webcam stream without necessarily sending a reciprocal stream means that it appears sometimes to be used for broadcasting pornography.

28. A survey was conducted, taking a single image from each of 323 user ids. 23 (7.1%) of those images contained undesirable nudity. From this we can infer that the true proportion of undesirable images in Yahoo webcam is $7.1\% \pm 3.7\%$ with confidence 95%.

# Advanced threats: Physical cables can be tapped

Trevor Paglen, NSA-Tapped Undersea Cables, North Pacific Ocean, 2016

# Physical/link layer threats

**Injection:** Violates integrity.

- Ethernet packets are unauthenticated: attacker who can inject traffic can create a frame with any addresses they like.

# Packet injection: ARP spoofing

- Recall: ARP used to map IP addresses to MAC addresses on local network

```
$sudo tcpdump -v -n -i eno1

tcpdump: listening on eno1, link-type EN10MB (Ethernet),
capture size 262144 bytes
17:29:47.455929 ARP, Ethernet (len 6), IPv4 (len 4), Request
who-has 172.16.15.1
        tell 172.16.15.151, length 46
```

- ARP requests broadcast to local subnetwork
- Anyone can send an ARP response
- Attacker on local network can impersonate any other host.

# Physical/link layer threats

**Jamming:** Violates availability.

- Physical signals can be overwhelmed or disrupted.
- Radio transmission depends on power and distance.

# Radio jamming: P25 law enforcement radios


Figure 1: Motorola XTS5000 Handheld P25 Radio

By careful synchronization, a jammer that attacks only the NID subfield of voice traffic can reduce its overall energy output so that it effectively has *more than 14dB of average power advantage* over the legitimate transmitter.

# Radio jamming: P25 law enforcement radios

Figure 1: Motorola XTS5000 Handheld P25 Radio

By careful synchronization, a jammer that attacks only the NID subfield of voice traffic can reduce its overall energy output so that it effectively has *more than 14dB of average power advantage* over the legitimate transmitter.


Figure 7: Girltech IMME, with modified firmware

While any CC1110 board for the correct frequency range is sufficient, we used the *GirlTech IMME*, a commercial toy intended for pre-teen children to text message one another without cellular service. Presently priced at $30 USD, the package includes a handheld unit and a USB adapter, either of which may be used with our P25 client (for an aggregate price of $15 per jammer).

Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System Clark et al. 2011

https://www.youtube.com/watch?v=NW-jRRTPCuw

# 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

Which attack happens where an attacker has sufficient access to observe and inject traffic which through timing/bandwidth is consumed by the victim before the legitimate reply arrives but cannot block packets?

A. Man on the side
B. Man in the middle
C. Physical access
D. Off-path
E. None of the above

Which attack happens when there is a third party that's monitoring and controlling a conversation between two parties, with the latter completely unaware of the situation?

A. SQL Injection
B. Man in the middle
C. Physical access
D. Off-path
E. None of the above

Which type of attack happens where a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network.

A. ARP Spoofing
B. DNS Spoofing
C. DHCP Spoofing
D. BGP Hijacking
E. None of the above

Which attack affects most ISPs and happens when attackers maliciously reroute Internet traffic.

A. ARP Spoofing
B. DNS Spoofing
C. DHCP Spoofing
D. BGP Hijacking
E. None of the above

**Conclusion:**

- Internet built from protocols that assumed trustworthy network operators.

- Next lecture: How to add security after the fact.