Application Layer Attacks & Countermeasures: DNS

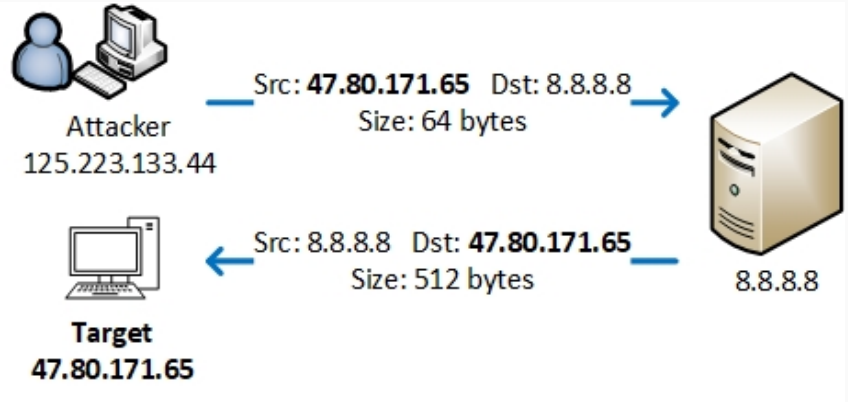
CYBR371: System and Network Security, (2024/T1)

Arman Khouzani, Mohammad Nekooei
Slides modified from "Masood Mansoori"

15 April, 2024

Victoria University of Wellington – School of Engineering and Computer Science

Reflection (and Amplification) Attacks: Characteristics



1. An unwilling intermediary is used to deliver the attack traffic.
    - Typically used in conjunction with spoofed Source IP address of the target.
    - The intermediary will deliver a response which will go to the target instead of the attacker.
    - Reflectors respond to the victim.
2. Attacks which make the victim service generate larger response than the trigger traffic.
    - Asymmetric attack, response is much larger than request.

Reflection (and Amplification) Attacks

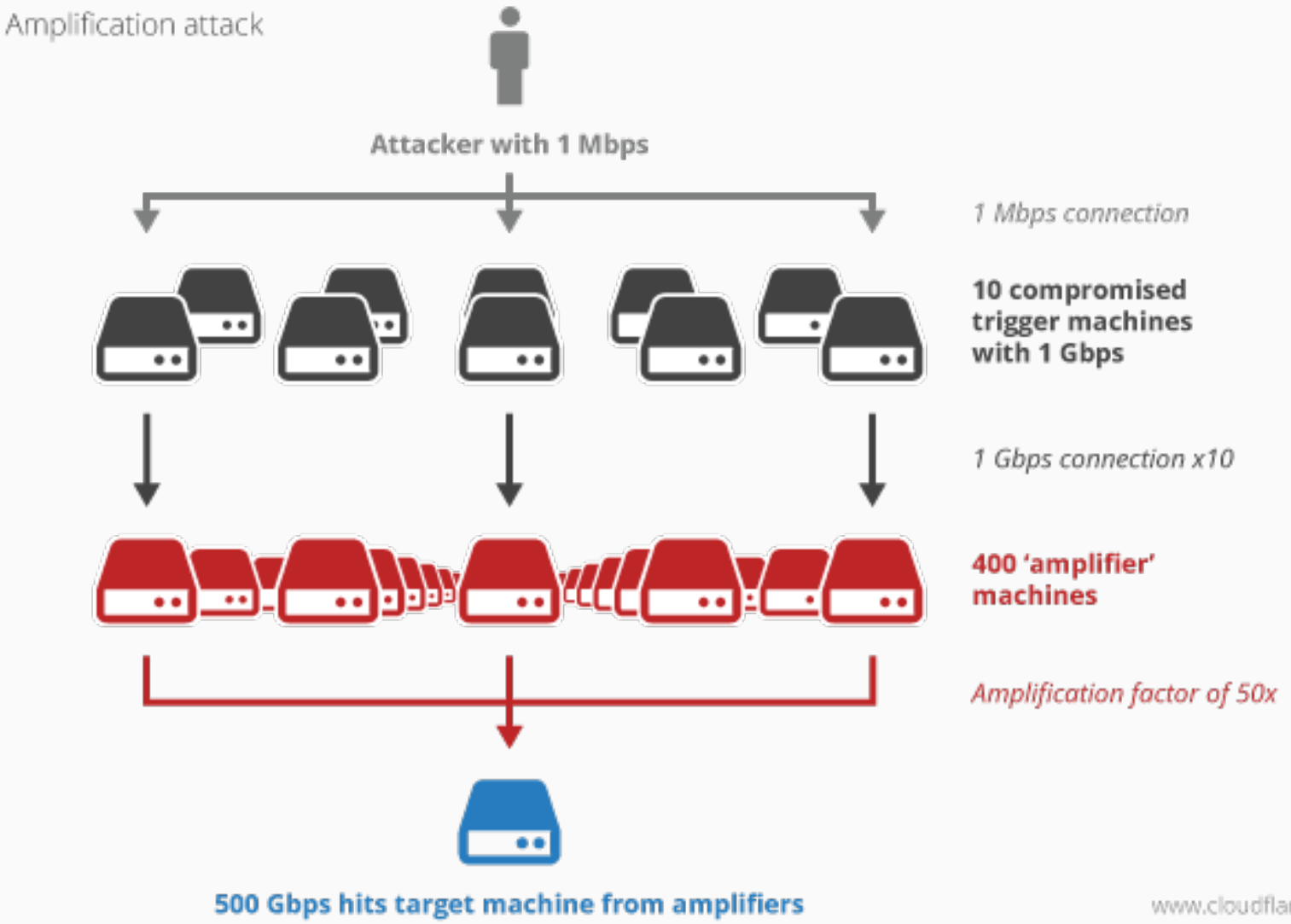
What protocols can we use for a reflection attack?

- **Domain Name System** (**DNS**)
  - Domain name to IP translation.
- **Network Time Protocol** (**NTP**)
  - Synchronising time.
- **Simple Service Discovery Protocol** (**SSDP**)
  - Discovery of network services.
- **Simple Network Management Protocol** (**SNMP**)
  - Exchanging management information between network devices.

DNS Reflection and Amplification Attack

Protocol	Bandwidth Amp. Factor	Vulnerable Command
DNS	28 to 54	Multiple
NTP	556.9	Multiple
SNMPv2	6.3	GetBulk Request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake	63.9	Server info exchange
Steam	5.5	Server info exchange

DNS Reflection and Amplification Attack

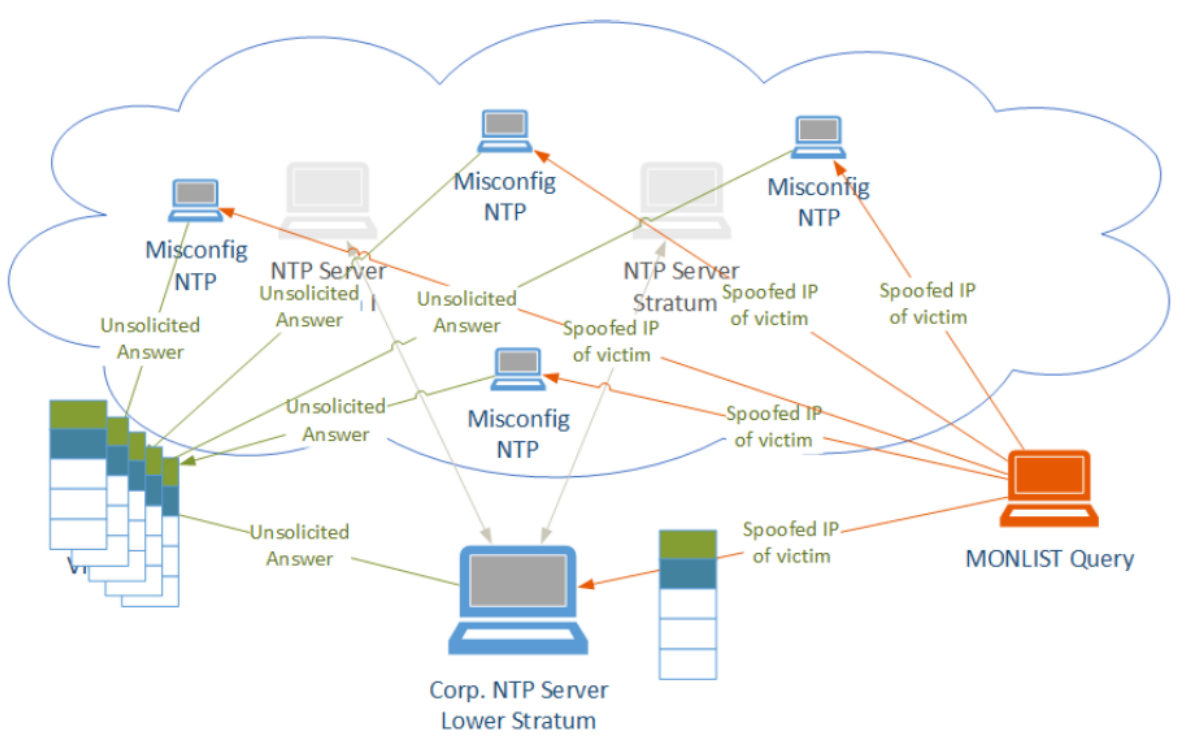


NTP Redirection and Amplification

NTP (**`Network Time Protocol`**) is used by machines connected to the Internet to set their clocks accurately.

Vulnerability to redirection and Amplification attack:

- It replies to every request packet without challenge
  - **`monlist`** command



NTP Redirection and Amplification Attack Mitigation

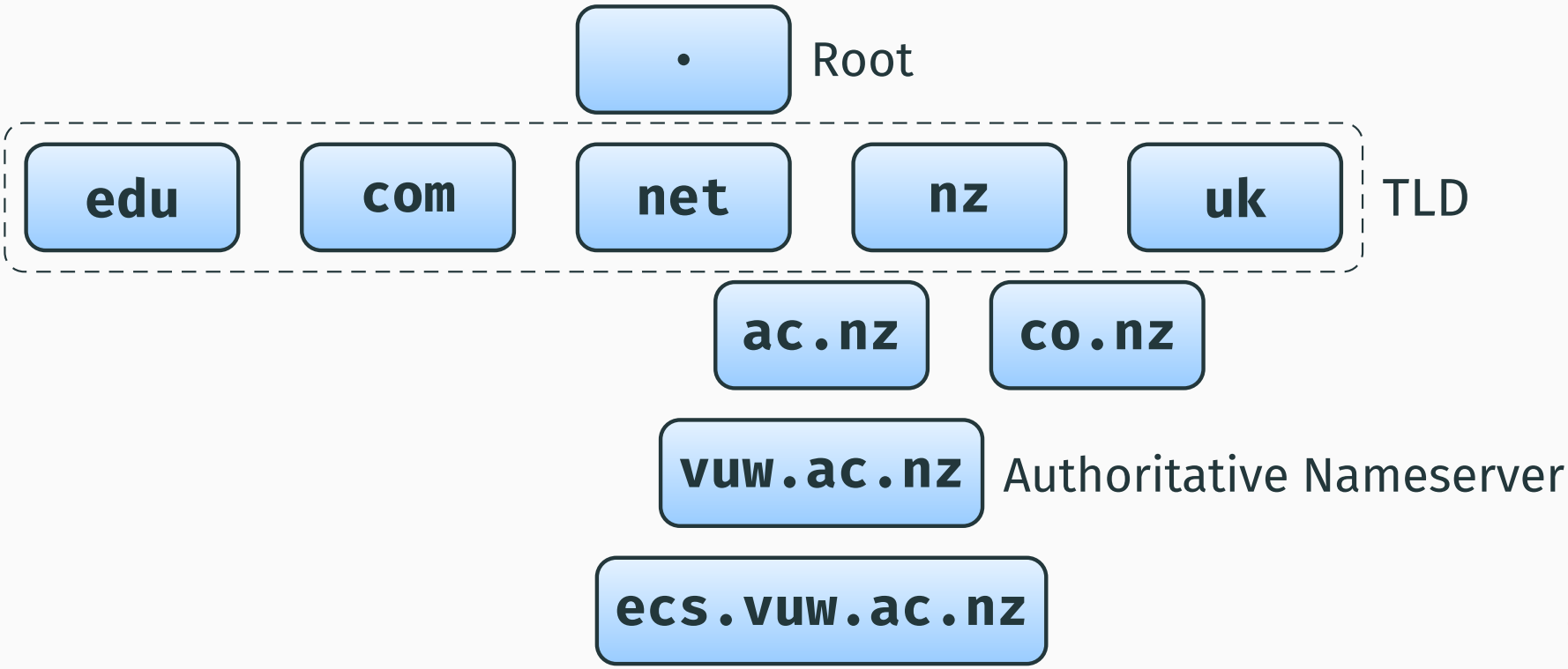
Countermeasures

1. Upgrading the server to the latest version
2. On the client
    - Filter port 123
    - Monitor NTP traffic
3. mrulist command vs monlist command
    - Requires Nonce:
        - Request Nonce: Initial request: 96-bit nonce specific to the requesting remote address, which is valid for a limited period.

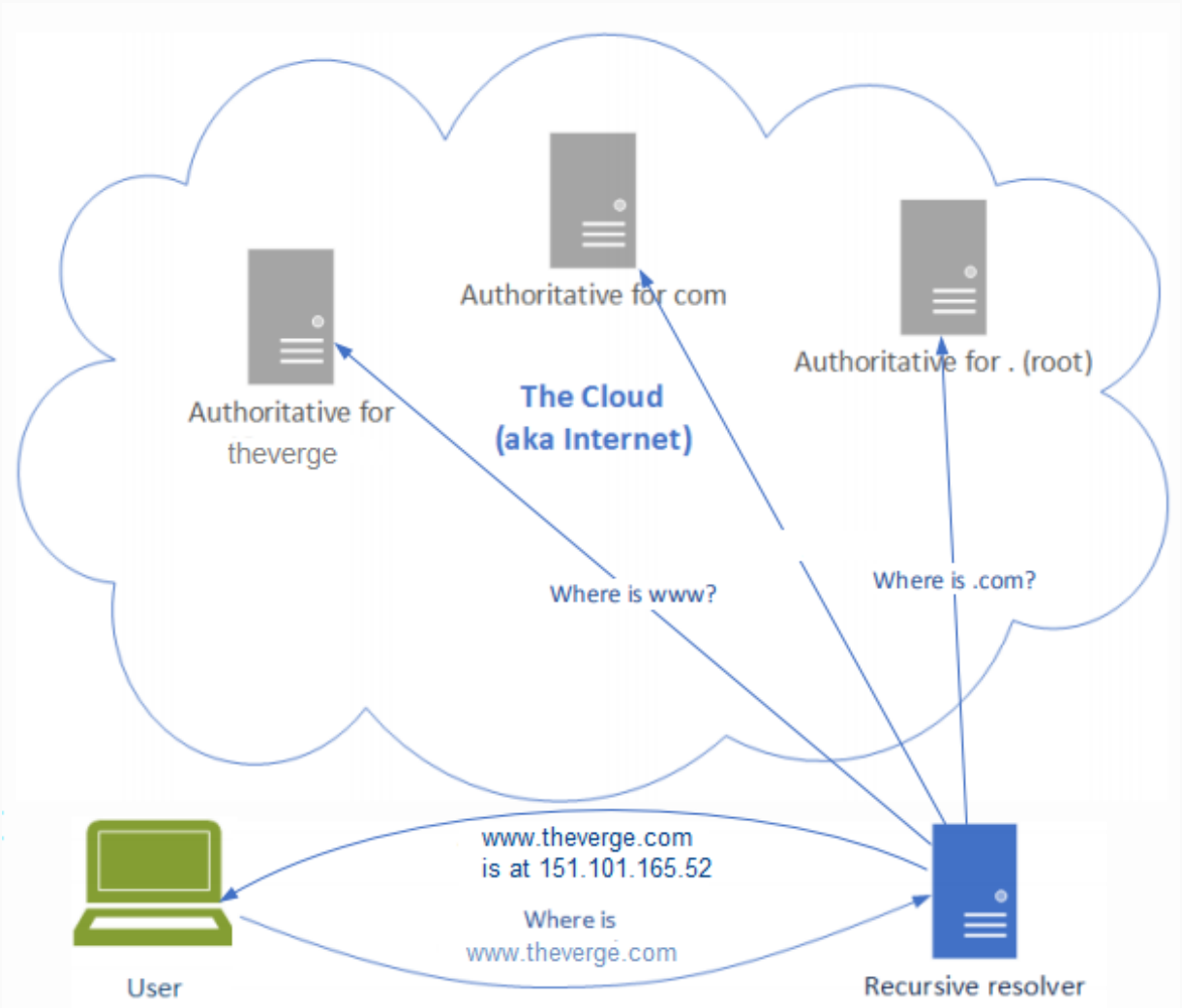
DNS Hierarchy

Top Level Domain (TLD)

- Country code Top Level Domain (ccTLD)
- Generic Top Level Domain (gTLD)
- Sponsored Top Level Domain (sTLD)

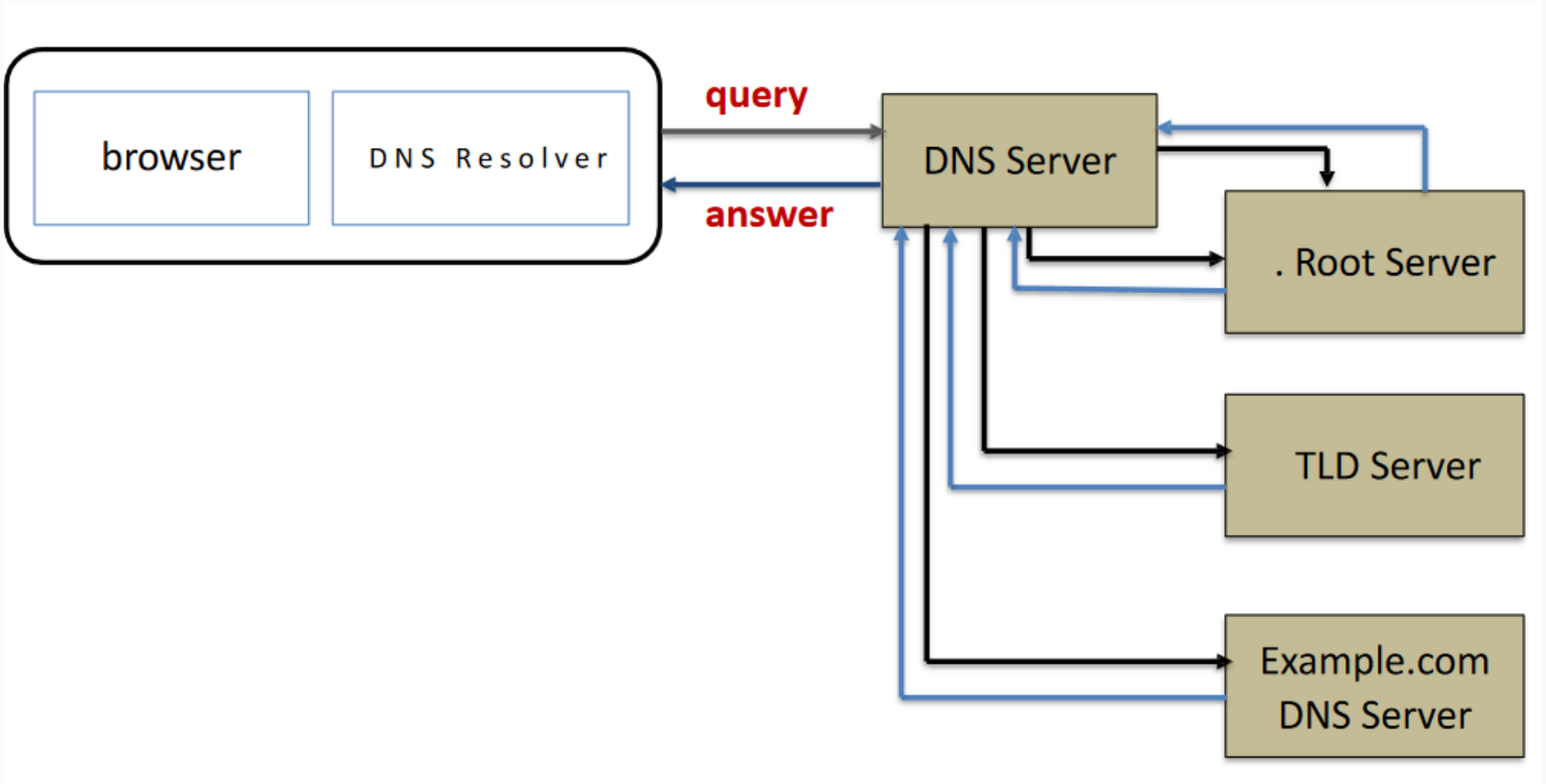


How does DNS Work?

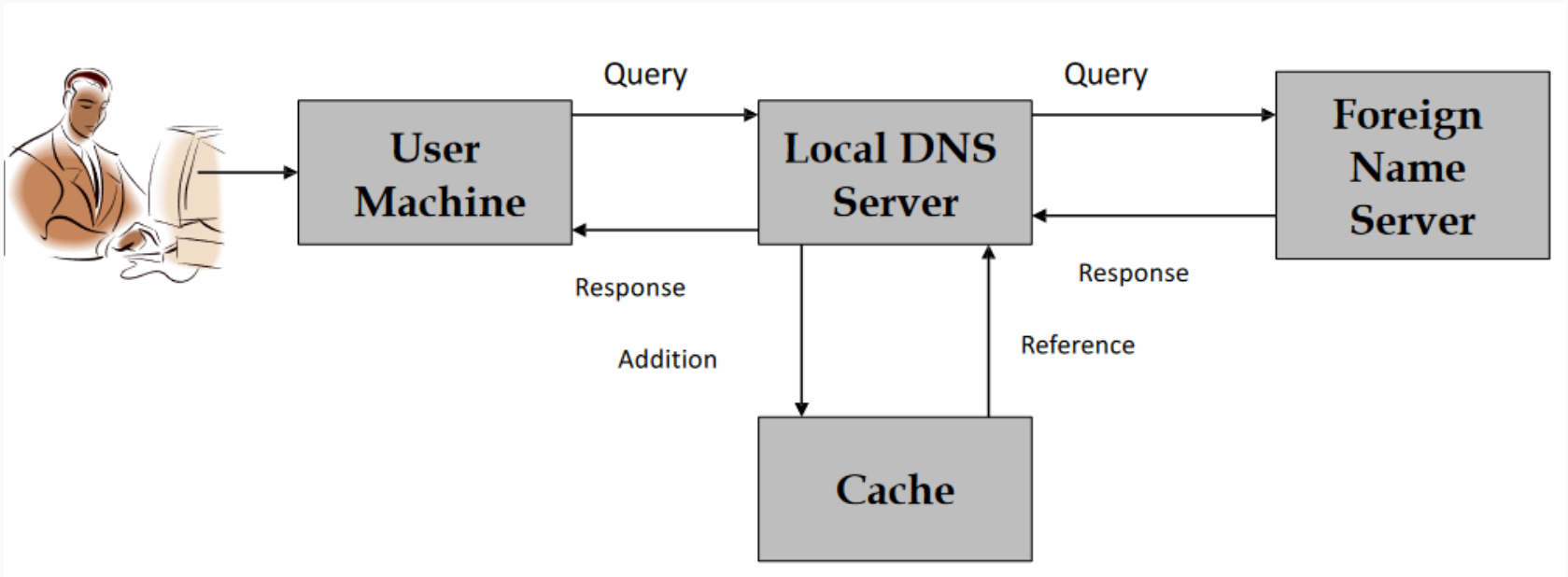


Who manages DNS root zones?

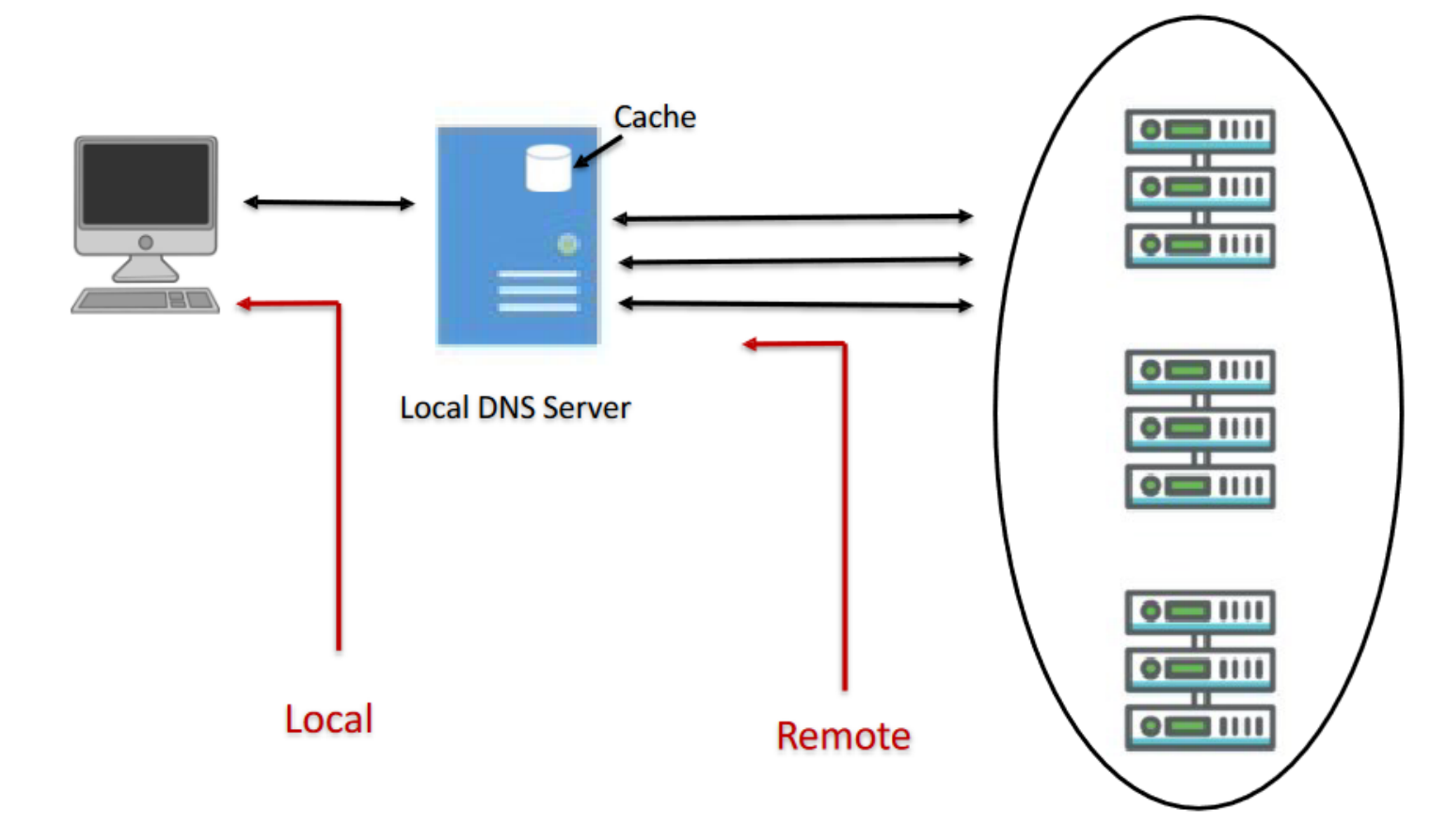
How does DNS Work?



How does DNS Work?

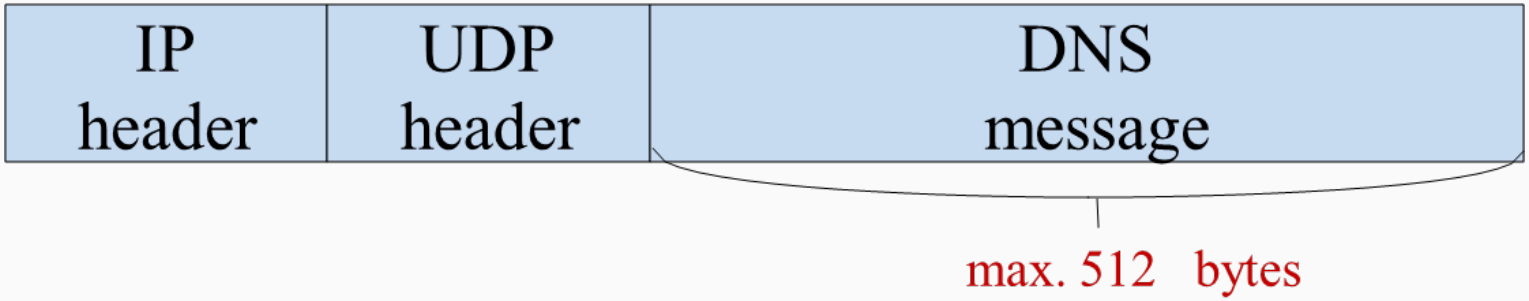


How does DNS Work?

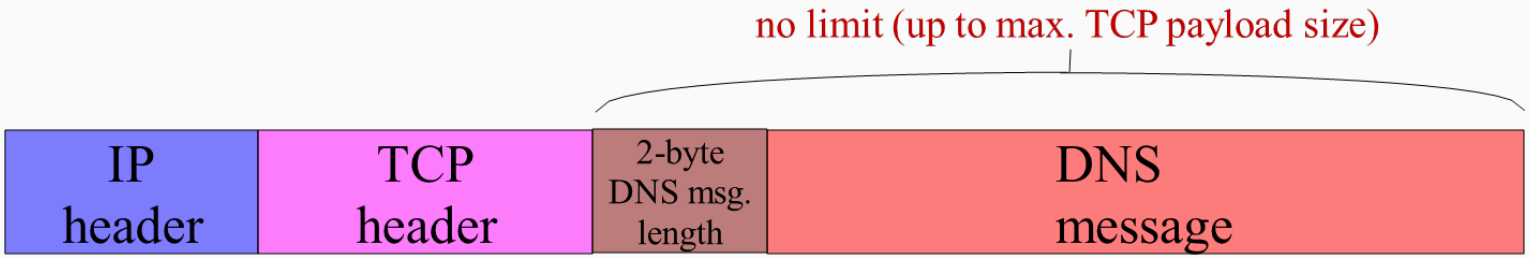


DNS Ports

DNS messages are encapsulated in UDP port 53 by default.



If the resolver expects the response to exceed 512 bytes, the resolver encapsulates the query in TCP (port 53) instead.



DNS Poisoning

Modify the client host file on the host (**`/etc/host`**)

- Takes precedence over DNS

Example:

IP Address	Hostname	Alias
127.0.0.1	localhost	deep.openna.com
208.164.186.1	deep.openna.com	deep
208.164.186.2	mail.openna.com	mail
208.164.186.3	web.openna.com	web

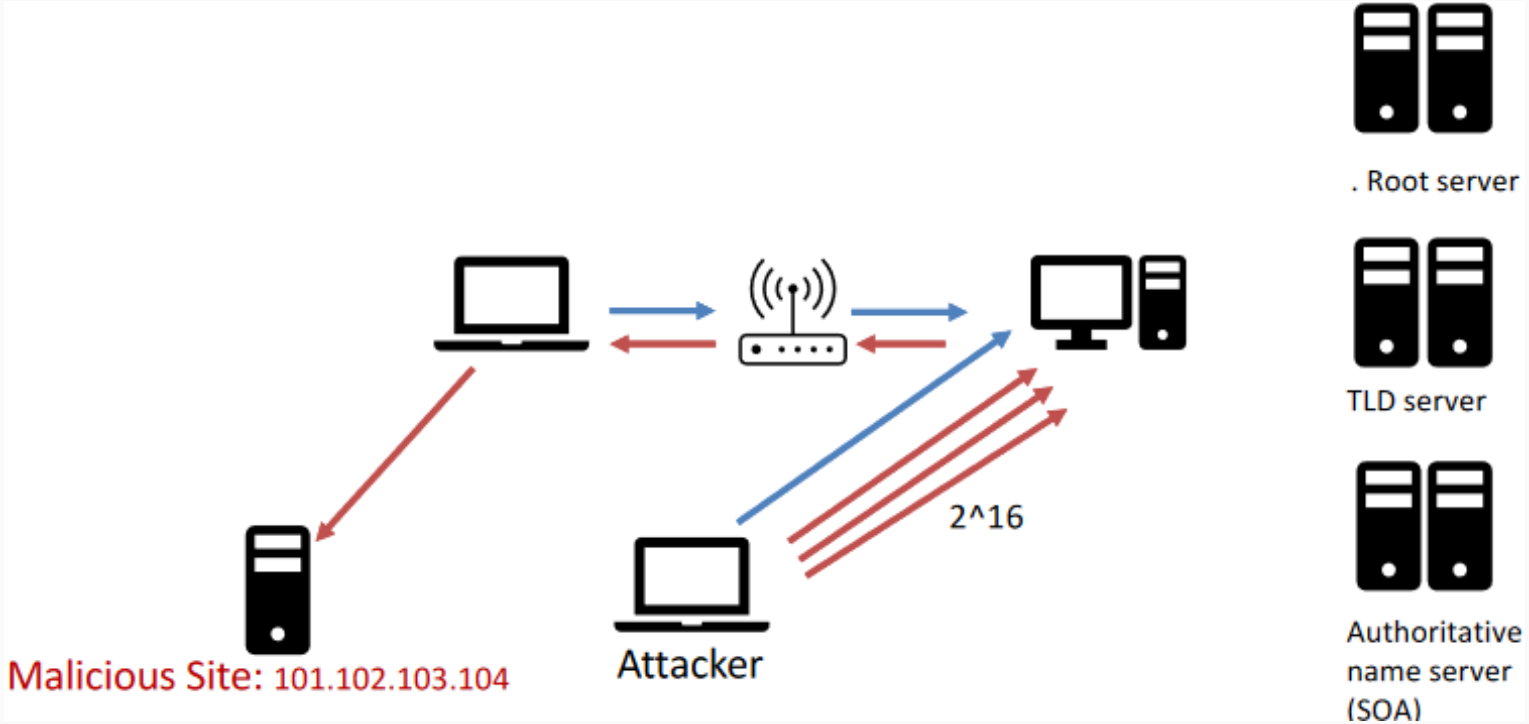
Local Cache Poisoning:

- Sniff request
- Spoof response (before reply from State Of Authority (SOA)

DNS Poisoning

Why wait for a client to make a request when we can make it ourselves?

- No need to race against SOA



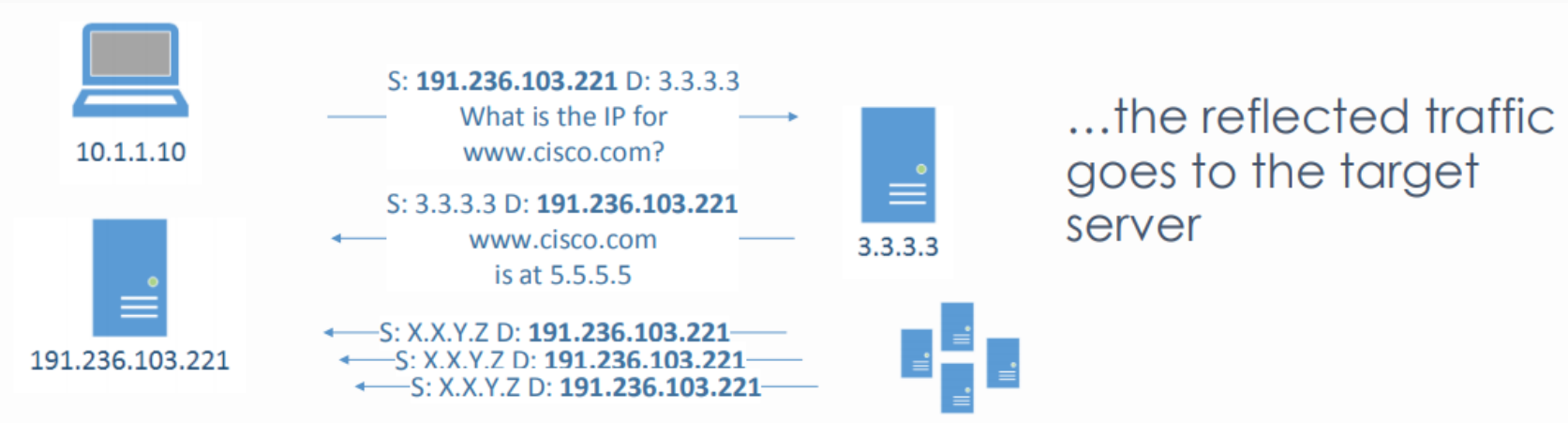
Countermeasures

- Partial fix: randomise query IDs
  - Problem: small space
  - Attack: issue a Lot of query
- Randomise source port number (don’t always use 53)
- DNSSEC (DNS Security Extensions):
  - Signatures to prove that answer is authentic
- HTTPS
  - Signatures to prove the website is authentic

DNS Reflection and Amplification Attack

What happens if an attacker spoofs the victim's IP address?

- and what if hundreds of misconfigured open DNS resolvers are used?



DNS Reflection and Amplification Attack

Consider the following query

`$ dig ANY us-cert.gov @8.8.8.8`

The response?

```
;; ANSWER SECTION:
us-cert.gov.            3599    IN      SOA     greyjoy.brass.us-cert.gov. hostmaster.us-cert.gov. 2020021201 120 60 604800 300
us-cert.gov.            0       IN      RRSIG   NSEC3PARAM 8 2 0 20200630000000 20200212203123 56448 us-cert.gov. Q1o80OkYAMnqvesQwDGJbj7FauwMxHdN6BjWKs4EesHp
e7aOoccfikL9 tD2/6gqjDpe8x9ev1SU+l9ItlQ2hUG21b8GShlBZWvIk3Yv7QaCHqdHv hb2oy38l9hviit/qbH/nlyvSwXOK0chNbkDJeo17BbE5DJtcDTFwrEz8 f7A=
us-cert.gov.            0       IN      NSEC3PARAM 1 0 10 C3612E
us-cert.gov.            299     IN      RRSIG   DNSKEY 8 2 300 20200630000000 20200212203123 56448 us-cert.gov. ADfI150xkWMrGatoDURXVs2gr370uXXLnVDMYH0ts3THYg
79fGnOLwx0 u/3gT9TRDVoGaUMjbSG9Q22xlYvPRIClHJfkkRGnoJmVrZ8hoVYT2zmw id3k8cqta+Voic2KoKKOzVJ6ctV16MbBudqFMMswwcB722rCi9fVWpUu A14=
us-cert.gov.            299     IN      RRSIG   DNSKEY 8 2 300 20200630000000 20200212203123 30121 us-cert.gov. XWjkIEnIMleWcYoubAT/qdRaNqhAw5NEeVhWCdb4YrOq8m
HHHRJijbkO ISBsa6vfJFklyxCHfRGYATPkg4Zh5z5ltLRX7tr8VwWAOmbglhyBAlgw k9qaJ1l3rhPYBUo8U5tIuaktvt0uVAD5c9xtm8/65YzSAUEfH4Pv95d7 pkc7RZAXDXfn7tz6aU1PkelRUnpFcSuXO
A4Xn7ZUO6Pg/8QSIpQRLojz BaVB0Bmzbx1fgQwzeSOZDmbOBwGbARzj1LAo2203vXPDqp71gMHnG9xO Wkhe8IrDyJzWUEdHc8SCRXu4WWcZygOahLBAkoeg7qRun2qdPggdG5Of F3aHrQF8zilZ8t7A+n79
sYiSwocm5dKYEgJibzV970j7ZBUWh7SULo4t rnuothF6SjznyVMKS+TPe7jDfVHmwV0X45+UPQZMdmGyao9cYKYoORKl 3THIBhCWijynk635qiihRJxtNgHf0WNjbd5brMtDraT2Eq6jnRuPmnhO 8mt9SYd
/GfVRGKowIVUHNkI7uCZSN5g+J3x4WFAPh5Amf4+uPNu+07AD F4Pi2mE2lv+/XcsMReeYjqVeZKzoMY7b8H2fvjJtGcjBFi743ppaaz28 YmTb59akMB1Ad60OK4vPZoPik+XzZXU9Q0Ei3SguDF1BpUdTKqG
D+qwQ gv5qXKitjCo=
us-cert.gov.            299     IN      DNSKEY  257 3 8 AwEAAbrkQMJMlq/wfwvwcohaQd1cMtYJVKBWpBPyI96VCFtdgslkaauB /HQ6Ac9l1jWve4N6ZR+KeLKWlLwiQqlFUI9cLBXMNxbvw
Pu7vUtGahL1 2VFUs501guS4/od7yhjp0EjDiJt0tu3AzYbMkHuZZiJZL3sFsOYOgtAj tKm/bJ4xq1rxpsWep9cQycj6XG3iu5RlPWVmn2x1TnHtR+kv+ZUK8nIq J92bZaVWn7C3aDTRY+3A7jYi16GkRi62
77i8I3xqDwzkqpQu9NMOUYpv 6xNEZqeBE/OpZvPTtBZJZExNm40kjPR/rTNf45QOCJ4KJsnDpnxLGqBi VPRzt4CbSAsHW0vMuiq4h+Fz/rpCzHorC3zi0/rsXgmwB4e0M7vw1XQ/ stxb64nJ8Uz8k7+piCF
mcohceKP6xO42z/61h7oh7iKHcJQxPjwtaW8s OfQQLzlXbh5zoU4+0adjGlcgNVEFNcsuEPMHvwDDUXXTpE/HlbRrMWGH KfIyaG1RBNlMBuUq1ZN88fxrlJR3xufm7dmCZBDYaQ0R27SZubofvN89 aKUwYs
50RIlgWb5d1qvVWMp/Llvh3nwdQ9bJJqw2XQSHhzjAL5sAh/3h mMBdLnr511vKd1HtGqtFavR8MqnkH5N0WbVr2jGzVl/KWFmaTNR9yzjB 3ltNWi8kB5n0mcor
us-cert.gov.            299     IN      DNSKEY  256 3 8 AwEAAZSo+yO9WJIiT+zLeOAFn963E2q5KvhU2ypOGKIi6sJv1KuFLShH 4Oin//4ZneKNOaruq4lC6+B/hRapTmn172vJauO8SCjFu
3+TtLTOD2ni /O5QVglWh/I40ySwiNdCchKE4GZeMY+8+kuQoeQ6D6bD3g7jYmwQFu3D Acoe7XkJ
us-cert.gov.            3599    IN      RRSIG   TXT 8 2 3600 20200630000000 20200212203123 56448 us-cert.gov. gd0d0GjcbOcmX+/LNZqsvlHMa3Mg4A12wlMJfk1V4Rr8as8+
AQGiiUGI WvBs+SM2mCxlgk+OoJHNa05SKhYc0OQbGm3C7xANjy3YZ4XPbdNlNIPj hX7EcstFoXTL3wkU2Cb31FmgaVggZMFtQ9xbqfJ1r710F4N2wdDG2U/M 3u4=
us-cert.gov.            3599    IN      TXT     "MS=ms22840512"
us-cert.gov.            3599    IN      TXT     "v=spf1 ip4:208.73.187.78/32 ip4:208.73.191.37/32 ip4:208.73.184.44/32 ip4:216.128.251.155/32 ip4:128.129.88.1
8/32 ip6:2620:112:5000:1::3/128 ~all"
us-cert.gov.            3599    IN      TXT     "d9a110e8d68b493995ac8e29a504a31d"
us-cert.gov.            3599    IN      RRSIG   MX 8 2 3600 20200630000000 20200212203123 56448 us-cert.gov. VC3OMNI3RsK7VBKS2TdBne91lI05lFHCM1RH/iDyOoC3Tjt+k
QPazYQO uQdR+tXn/hpBdd/mCcfrZK9fSKXKqpsJX1+I9KTVoQNUaHKwuDzbwOqs K5437B/eSIW/B7dNBvPxK8DvKDCMSpIkE4l6IKV6WIXYdxB7Vs7KN+CT LoU=
us-cert.gov.            3599    IN      MX      10 smtp2.us-cert.gov.
us-cert.gov.            3599    IN      MX      10 smtp3.us-cert.gov.
us-cert.gov.            3599    IN      MX      10 smtp4.us-cert.gov.
us-cert.gov.            3599    IN      MX      10 smtp1.us-cert.gov.
us-cert.gov.            3599    IN      RRSIG   A 8 2 3600 20200630000000 20200212203123 56448 us-cert.gov. AXVlDKc5qR/cEIpHBWkQHM95n+9wp5Fc5/WHOR/XAb92X1tf+S
dYXe1v glolGUKn9AGwVKo2yeFE0cMU5O4qJ90jJ76bnogF/xcAUljg90GfBy1q 9YVJtqiSdZrbKwIH6ioxkXL1wUtAJKSPWTZMbvblvWwuuZlDAw191koR 6Ik=
us-cert.gov.            3599    IN      A       173.252.133.166
us-cert.gov.            3599    IN      RRSIG   NS 8 2 3600 20200630000000 20200212203123 56448 us-cert.gov. ktiO8GVcsyZ4HcfJWDK9W7UChjGizQJ7cabw/+wB4BNHoIgzu
4OmIoUh o8ABqXqc3+leMv9EluBN62TOU+/3QxZtdsYIVrKOTC/artTEwd7RRvOK sMqrVsOejXYQLCqoBXGU+M0Ao8pgcVZQTELLjHyDTSDRYRmRS1CUKqV9 E0M=
us-cert.gov.            3599    IN      NS      greyjoy.brass.us-cert.gov.
us-cert.gov.            3599    IN      NS      stark.brass.us-cert.gov.
us-cert.gov.            3599    IN      RRSIG   SOA 8 2 3600 20200630000000 20200212203123 56448 us-cert.gov. JfVpuJPT3Eus0wA+1IBVznA9xd070/b+YT/jRl7RqHw6Yf/m
4JJYv1jI SrG7/U2FSERQGpzapU/wHkbjEImOD9lThbhITbrPWKPVvpKeRHIz6zfn UCbKKxgVdTrGl3lk0likkY3R7DTPrmWDa/RnDnOWoXE6hVfA3I3O+HRh 3Bs=
```

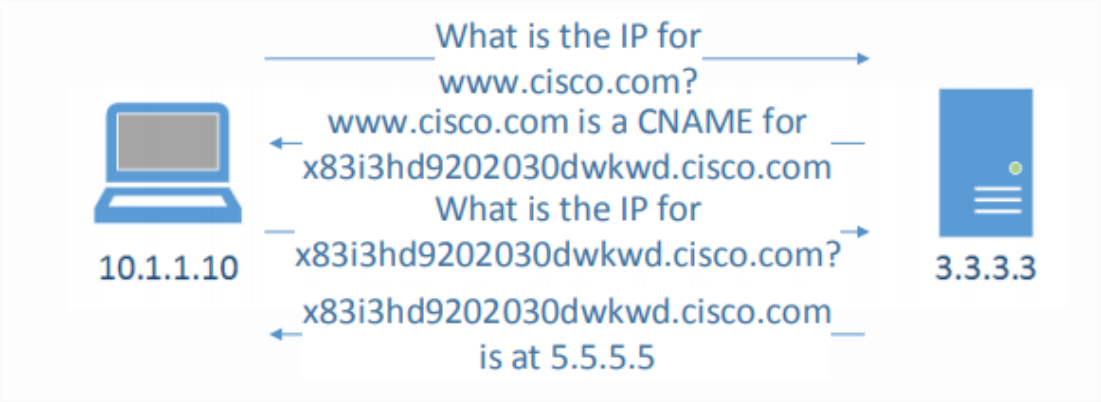
DNS Reflection and Amplification Attack

DNS amplification and spoofing.

No.	Time	Source	Destination	Protocol	Info
9784…	274.574542	8.8.8.8	130.195.9.141	DNS	Standard query response 0x13e8 ANY ieee.org
9784…	274.575295	8.8.8.8	130.195.9.141	DNS	Standard query response 0x13e8 ANY www.amazon.com
9784…	274.575342	8.8.8.8	130.195.9.141	DNS	Standard query response 0x13e8 ANY www.yahoo.com CNAME atsv2-fp-shed.wg1.b.yahoo.com
9784…	274.577314	8.8.8.8	130.195.9.141	DNS	Standard query response 0x13e8 ANY ietf.org
9784…	274.577365	8.8.8.8	130.195.9.141	DNS	Standard query response 0x13e8 ANY www.yahoo.com CNAME atsv2-fp-shed.wg1.b.yahoo.com
9784…	274.579067	8.8.8.8	130.195.9.141	DNS	Standard query response 0x13e8 ANY ieee.org
9784…	274.579546	8.8.8.8	130.195.9.141	DNS	Standard query response 0x13e8 ANY www.amazon.com
9784…	274.580761	8.8.8.8	130.195.9.141	DNS	Standard query response 0x13e8 ANY www.amazon.com
9784…	274.581113	8.8.8.8	130.195.9.141	DNS	Standard query response 0x13e8 ANY ietf.org
9784…	274.581846	8.8.8.8	130.195.9.141	DNS	Standard query response 0x13e8 ANY ieee.org
9784…	274.582587	8.8.8.8	130.195.9.141	DNS	Standard query response 0x13e8 ANY www.amazon.com
9784…	274.582658	8.8.8.8	130.195.9.141	DNS	Standard query response 0x13e8 ANY ieee.org
9784…	274.582705	8.8.8.8	130.195.9.141	DNS	Standard query response 0x13e8 ANY www.yahoo.com CNAME atsv2-fp-shed.wg1.b.yahoo.com
9784…	274.582804	8.8.8.8	130.195.9.141	DNS	Standard query response 0x13e8 ANY ietf.org
9784…	274.582884	8.8.8.8	130.195.9.141	DNS	Standard query response 0x13e8 ANY ieee.org
9784…	274.582884	8.8.8.8	130.195.9.141	DNS	Standard query response 0x13e8 ANY www.amazon.com
9784…	274.582921	8.8.8.8	130.195.9.141	DNS	Standard query response 0x13e8 ANY www.amazon.com

DNS DoS Attacks Mitigation

- Validate packet and query structure
- Whitelisting
- ”Challenges”: Establish the requester’s identity before sending a full answer.



Challenges with DNS challenge?

- Two times the amount of traffic
- Two times the packet rate
- Computational resources

HTTP Attacks and Mitigation

The **`Hypertext Transfer Protocol`** (**HTTP**) is an application-level protocol and generally works over TCP, or over an encrypted TCP connection.

HTTP is a client-server protocol:

- Requests are sent by the user-agent (browser - or a proxy on behalf of the client).
- Each individual request is sent to a server, which handles it and provides a response.

Attacks:

- http GET attack
- http POST attack

Countermeasures?

Next: Firewalls