Network Security Course | ETH Zurich - Autumn 2020

DNS Security

Dr. Stefan Frei

Security Officer @ SIX Digital Exchange www.sdx.com
frei@techzoom.net | Twitter @stefan_frei

Head of the working group "Supply Chain Security" @ ICT Switzerland

The Internet is a critical infrastructure

Its operation depends on the fundamentally insecure DNS

Domain Name System (DNS) Security

The security of DNS is critical to the security of the Internet

Manipulating the DNS mapping allows an attacker:

- To redirect connections to divert users to a malicious server
- To facilitate Man-in-the-Middle (MitM) attacks
- To launch denial of service (DoS) attacks

WHY?

- Know DNS from attackers and defenders perspective
- Recognize security impact of specific protocol features
- Recognize how complexity favors attacker in surprising ways

MORE WHY?

- Use DNS as an example to explain and understand classes of attacks

Domain Name System (DNS)

DNS has become a formidable attack vector for criminals

DNS OBJECTIVE

- Provides a mapping of names to resources of several types
- E.g. resolve domain name `www.ethz.ch` to IP address `129.132.19.216`

ATTACKERS PERSPECTIVE

- Is a freely available distributed storage system
- Can also be (ab)used to stream audio and video
- Is abused for powerful denial of service attacks
- Is abused for various impersonation attacks
- Used to setup services that are hard to hunt-down or shut-down (Botnets, Fast- & Domain Flux)

It is essential for defenders to understand DNS and how it is used and abused by cyber criminals

DNS Key Properties

A distributed global lookup mechanism for translating names into other objects

DNS MODEL

- DNS is a *globally distributed*, *loosely coupled*, *scalable*, *reliable,* and *dynamic database*
- DNS data us *maintained locally* and *retrievable globally*
- No single computer has all DNS data

NAMESPACE

Hierarchical namespace defines names and ownership

- Root > Top level domains > Second level domains

SERVER

Make namespace available and store data

- Authoritative & recursive Forwarders

PROTOCOL

Simple protocol

- TCP or UDP Port 53
- No built-in encryption, integrity, authentication

RESOLVERS

Clients to query servers

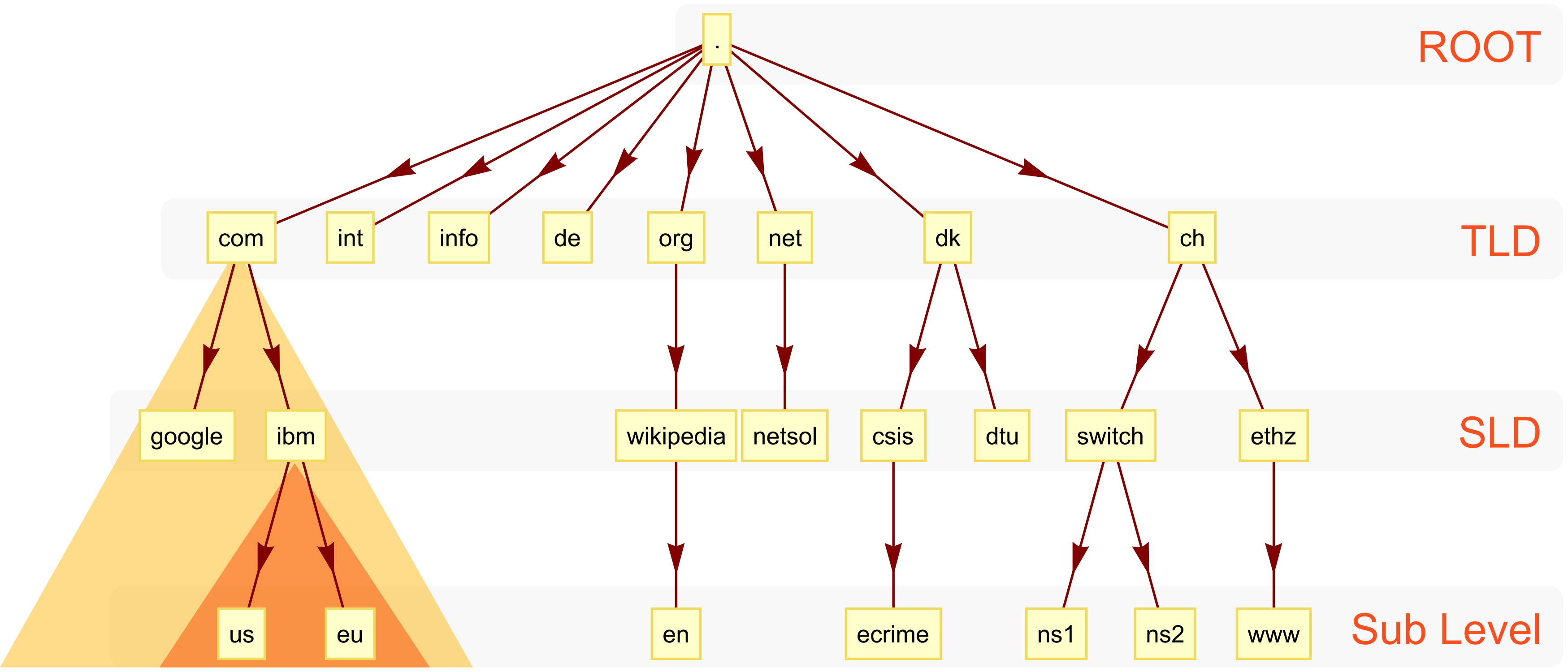
- Query servers
- Processes to resolve names

DNS Namespace

A distributed global lookup mechanism for translating names into other objects

Hierarchical namespace

- Tree structure down from **root** level "." for scalability
- Below root are top-level domains (**TLD**) e.g. .com, .ch
- Below the TLD are second-level domains (**SLD**) e.g. ibm.com, ethz.ch



Controlled by IANA (US Department of Commerce)

Controlled by specific domain registrars (selected by IANA)

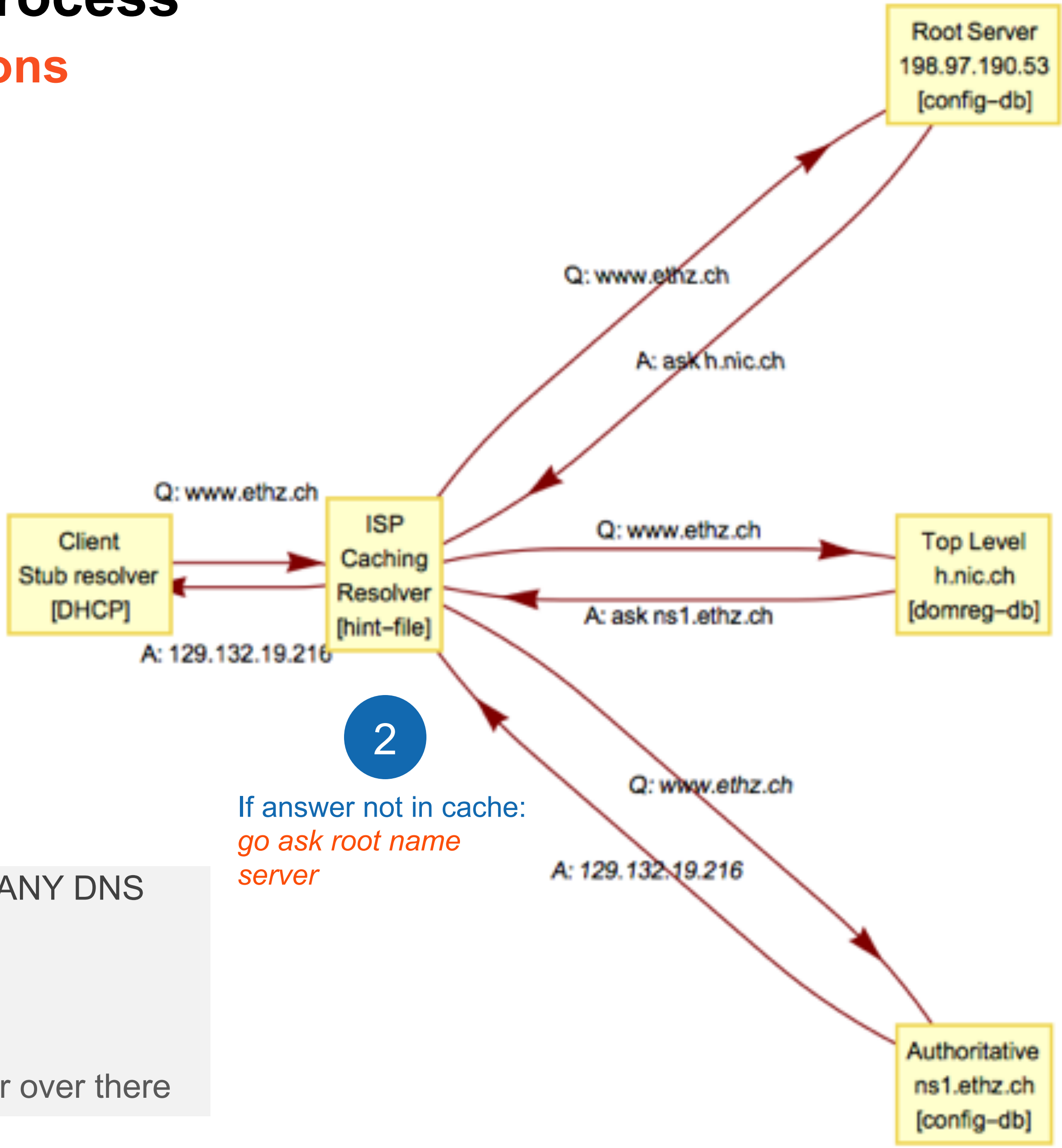
Owned and managed by private entities

Owned and controlled by SLD owner

DNS - Resolution Process

A hierarchy of delegations

1 **What is the IP of www.ethz.ch?**



2 If answer not in cache:
go ask root name server

3 Root Server Reply:
go ask top-level name server

4 Top Level Domain Server Reply:
go ask authoritative name server

5 Authoritative Server Reply:
I have the info, here is the IP address requested

THREE POSSIBLE ANSWERS TO ANY DNS QUESTION:

1. Here's your answer
2. Invalid request - go away
3. I don't know, ask that name server over there

DNS
Protocol Features

DNS Protocol

Key Protocol Features

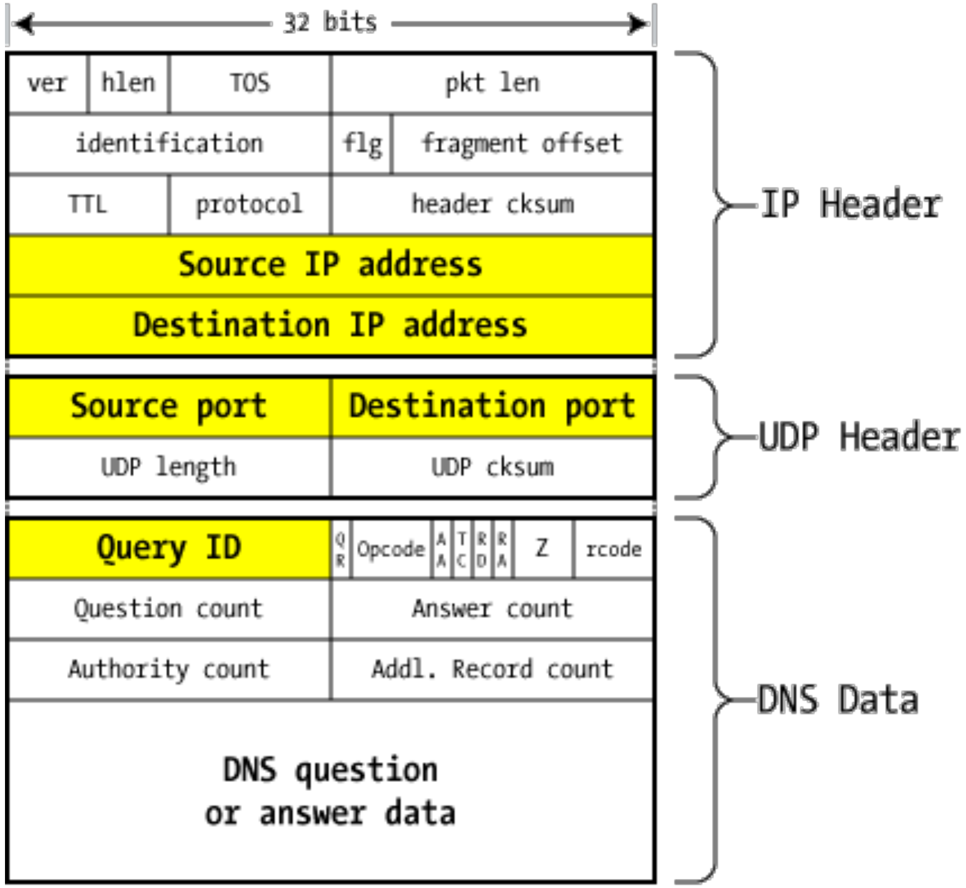
The DNS protocol was designed with a mechanism to protect against forged responses. The first two bytes in the message form a **transaction ID** txid that must be the same in the query and response.

FEATURES

- **Network:** TCP / UDP Port 53
- **Query:** Client sets the query and a random txid
- **Response:** Reply includes query, txid , and response

SECURITY

- Client expects txid to match (else drops response)
- Random txid introduces 16 bit of entropy: 2^{16} = 65,536
- Random source port introduces max 16 bit of entropy
- NO CONFIDENTIALITY
- NO INTEGRITY VERIFICATION
- NO AUTHENTICITY



DNS Record Types

Resource Records (RR) define data types in the Domain Name System (DNS)

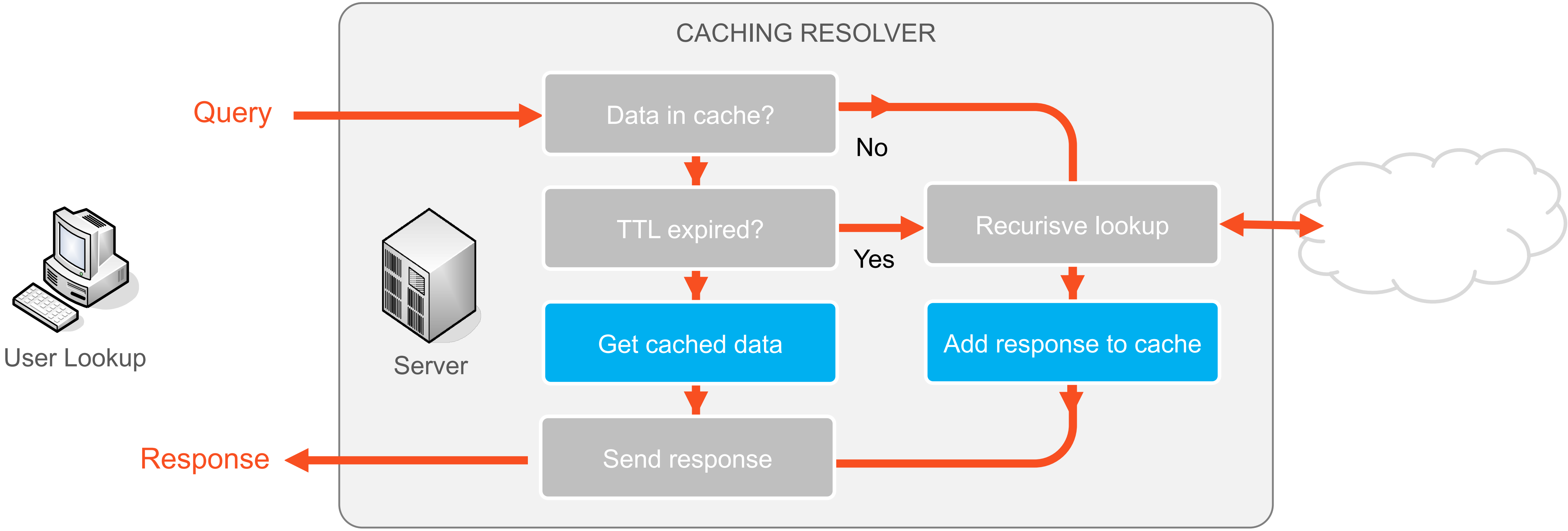
RECORD TYPE	DESCRIPTION	USAGE
A	ADDRESS RECORD	Maps FQDN into an IP address
PTR	POINTER RECORD	Maps an IP address into FQDN
NS	NAME SERVER RECORD	Denotes a name server for a zone
SOA	START OF AUTHORITY RECORD	Specifies many attributes concerning the zone, such as the name of the domain (forward or inverse), administrative contact, the serial number of the zone, refresh interval, retry interval, etc.
CNAME	CANONICAL NAME RECORD (ALIAS)	Defines an alias name and maps it to the absolute (canonical) name
MX	MAIL EXCHANGER RECORD	Used to redirect email for a given domain or host to another host
TXT	TEXT RECORD	free form text of any type, e.g. Sender Policy Framework (SPF), or and DomainKeys Identified E-mail (DKIM)

Source: https://www.ietf.org/rfc/rfc1035.txt

DNS Caching

DNS resolution is a complex and time consuming process

- Caching: We want to decrease lookup latency and network traffic
- Cache expiration controlled by time-to-live TTL
- Cache positive (content) and negative (nxdomain) results



Attack Patterns

How could you attack DNS

ATTACKER OBJECTIVE

- Insert tampered information into DNS server or resolution process
- Control DNS of all clients serverd by name server / resolver

WHY DO WE INVESTIGATE THIS?

- We use DNS protocol and features to explain attack classes, irrespective of protocol (e.g. cache poisoning, session state, ..)
- Understand security impact of specific features in protocol design or implementation

As is often the case in cyber security, old attacks become new again:

DNS cache poisoning was exploited and solved in

- **1995** (Paul Vixie)
- **2000** (txid randomization)
- **2008** (Dan Kamisky)
- **2020** (Keyu Man - SADDNS)

Source: https://www.saddns.net

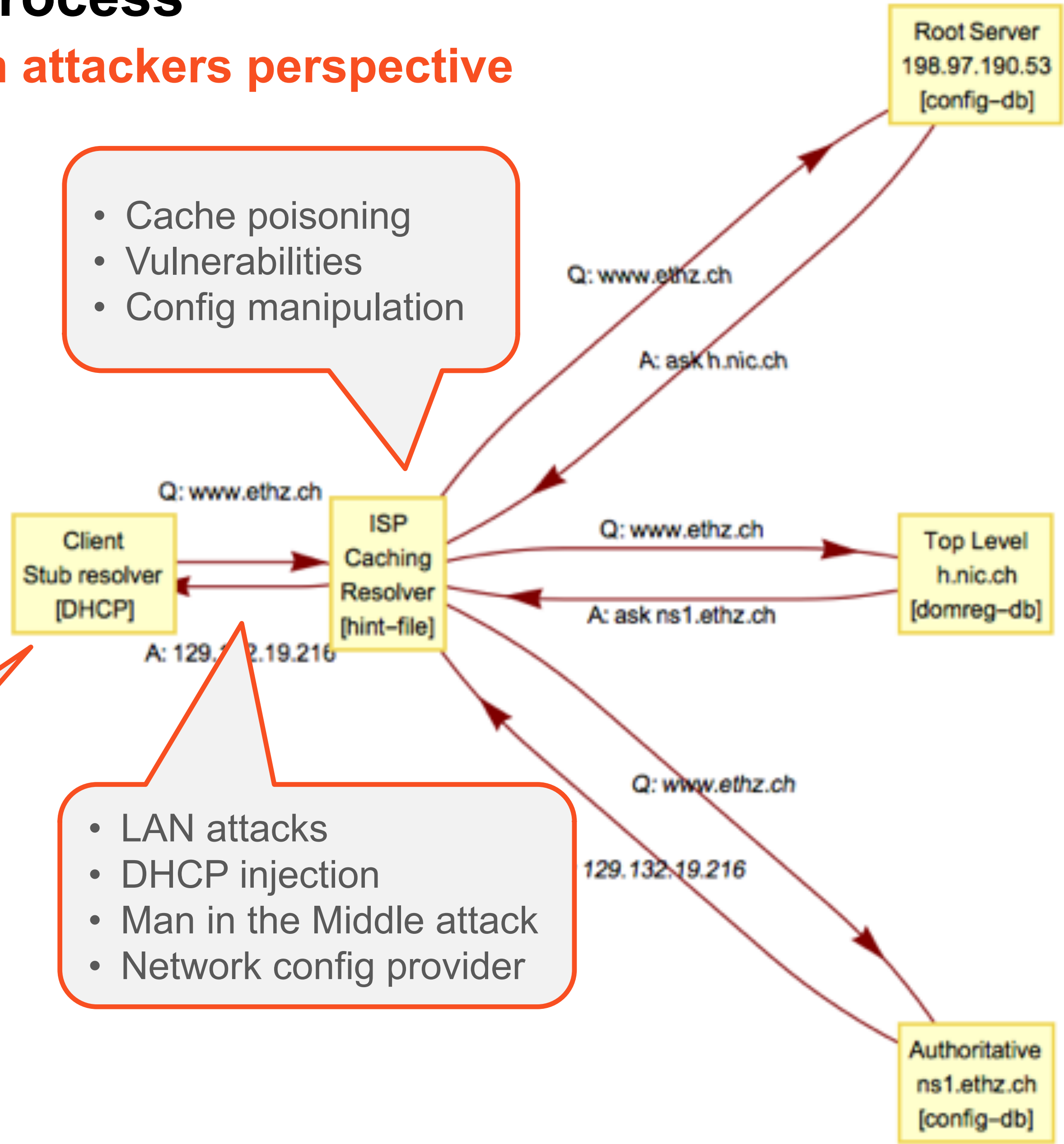
DNS - Resolution Process

DNS resolution from an attackers perspective

- Cache poisoning
- Bogus DNS config
- /etc/hosts entries
- Malware

- Cache poisoning
- Vulnerabilities
- Config manipulation

- Compromised domain registrar
- Compromised client account at registrar
- Vulnerabilities / passwords



- Cache poisoning
- Bogus DNS config on router/modem

- LAN attacks
- DHCP injection
- Man in the Middle attack
- Network config provider

- Compromised name server
- Vulnerabilities / passwords
- Config manipulation

Common DNS Attacks

LOCAL HOST NETWORK	▪ Manipulate DNS entries and conversation on local host or network ▪ Impact: impersonation of services
CACHE POISONING	▪ Inject manipulated information into DNS cache of resolver ▪ Impact: impersonation of services
DNS TUNNELING	▪ Uses DNS as a covert communication channel to bypass firewalls ▪ Impact: Data exfiltration and hidden communication
DNS HIJACKING	▪ Modify DNS record settings (most often at the domain registrar) to point to a rogue DNS server or domain ▪ Impact: impersonation of services
DISTRIBUTED REFLECTION	▪ Abuse large number of DNS servers to combine reflection and amplification of queries. ▪ Impact: DDoS on victim

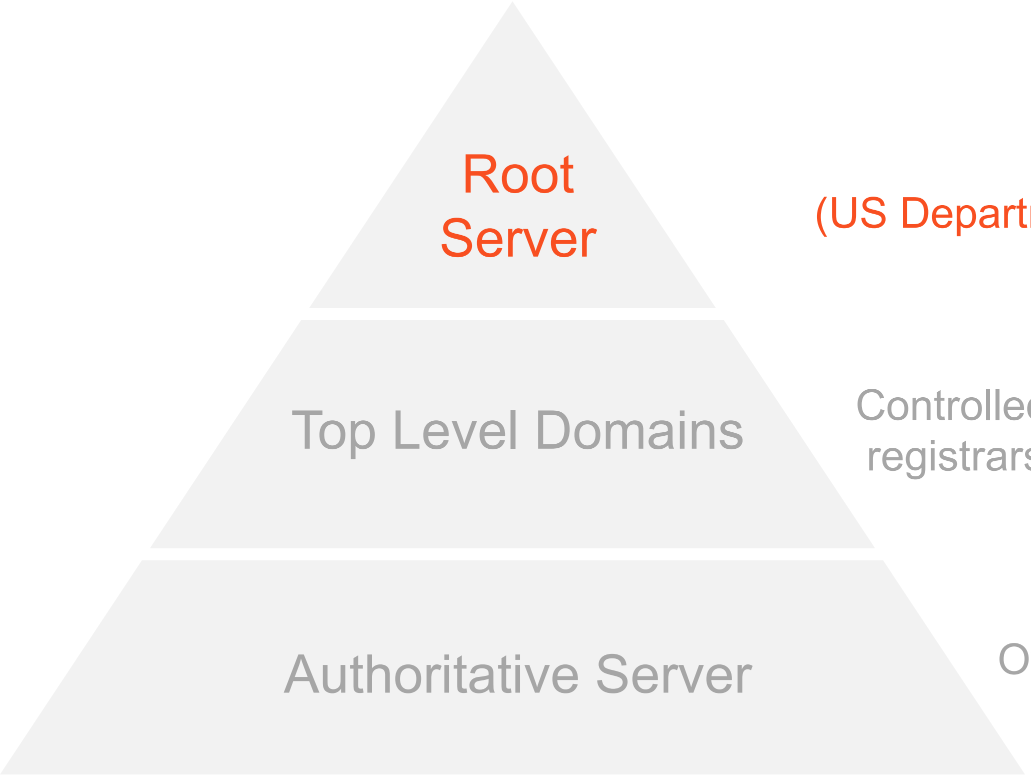
DNS
Root Server Security

DNS Root Zone

DNS root name servers are the key to the Internet kingdom

The DNS root zone is served by 12 root server clusters which are authoritative for queries for the **top level domains.**

Every name resolution in the Internet either starts with a query to a root server, or, uses information that was once obtained from a root server



Controlled by IANA (US Department of Commerce)

Controlled by specific domain registrars (selected by IANA)

Owned and managed by private entities

DNS ROOT NAME SERVERS

- Have the official names a.root-servers.net to m.root-servers.net
- Only resolve the IP addresses for the top-level name servers (TLD)

All other name servers use a hard coded config file to lookup the IP addresses for the root name servers (hints-file [1])

[1] https://www.iana.org/domains/root/files

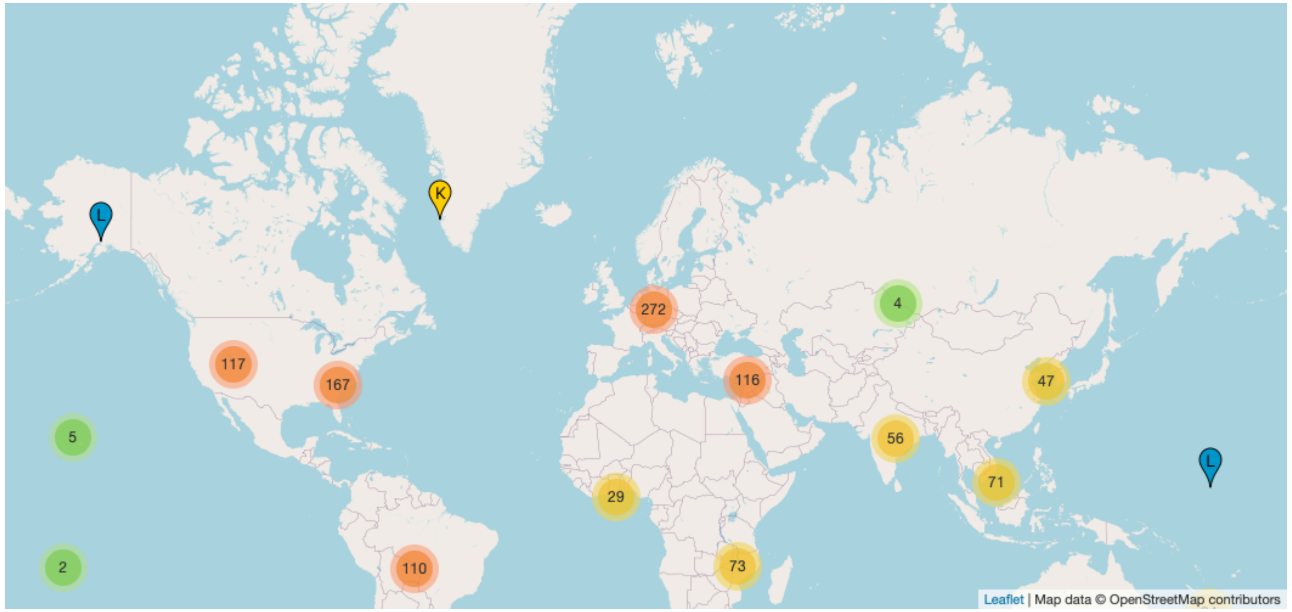
Root Server System (RSS)

The RSS resolution process and its security can affect all users of the Internet.

The root server system (RSS) consists of 1,342 instances operated by the 12 independent root server operators (RSO)

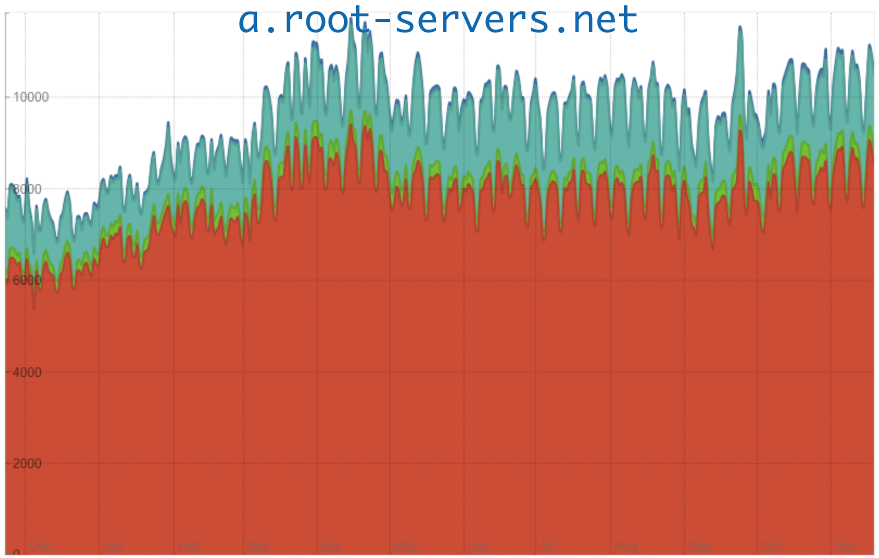
- Availability and data integrity of the root zone are the primary concerns
- The diversity of independent RSO with individual mitigation strategies lessen the threat of various attacks

Root Server Operators



Query Volume

4 to 12 Billion queries per day



Dec 19 Nov 20

Source http://www.root-servers.org

Root Server System (RSS)

Key Challenge: Denial of Service Attacks (DOS)

A sophisticated (D)DoS attack could saturate any system on the Internet. The bandwidth available at RSS is significant, but not immune to DoS

DOS ATTACK ON
NETWORK BANDWIDTH

Mitigation

- Localize attacks and **limit their effects close to the sources** of traffic.
- Hundreds of root servers deployed **across different ISPs around the world**.
- RSS is **heavily anycasted.**
- RSO with **hundreds of upstream providers** and private peers.

DOS ATTACK ON
MEMORY & CPU

Mitigation

- Replication of the RSS among multiple operators and thousands of machines
- System monitoring allow for quick detection of attacks, and (automated) actions

Challenge: DNS Enhancements

- DNS-over-HTTP (DoH) and DNS-over-TLS (DoT) shift traffic towards TCP with additional overhead for cryptographic operations and protocol parsing

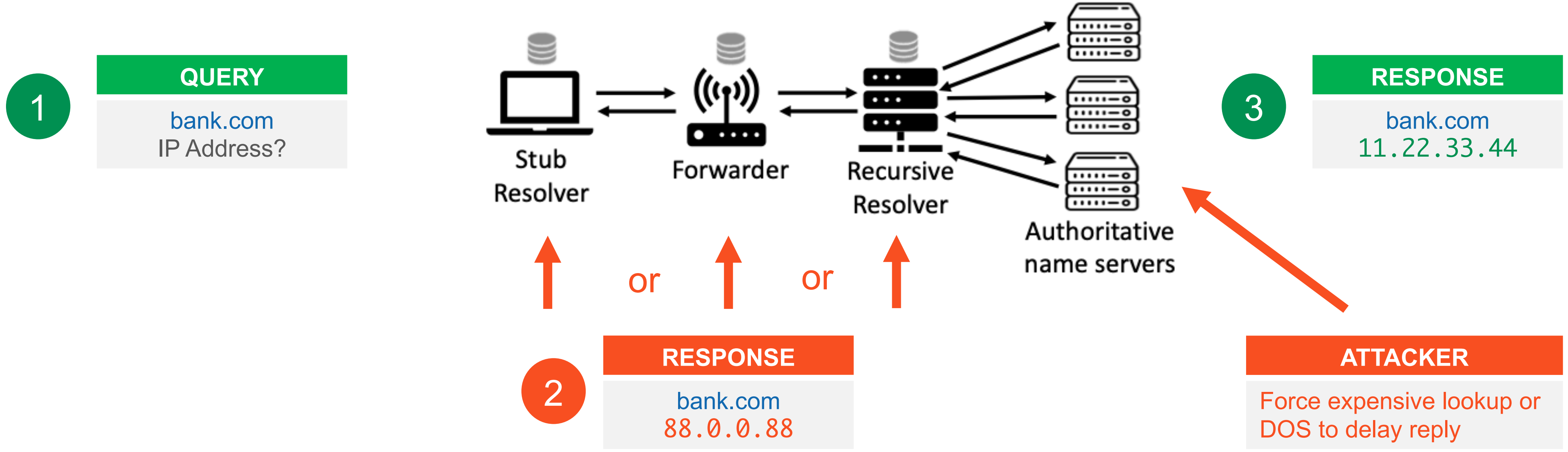
More threats: https://root-servers.org/media/news/Threat_Mitigation_For_the_Root_Server_System.pdf

ETH zürich

Attack Pattern
Cache Poisoning

Attack Pattern - Cache Poisoning

Attacker inserts incorrect resolution information



ASSUMPTION
- The attacker is off-path (not able to eavesdrop traffic between a forwarder and resolver)
- If required, the attacker could make client to resolve a FQDN the attacker controls

PREREQUISITE
To inject a fake response, the attacker needs to
- Reply faster - before true response arrives
- Guess the correct src / dest IP, src / dest port, and the transaction ID of the query

Source: https://dl.acm.org/doi/pdf/10.1145/3372297.3417280

Cache Poisoning - Implementation Vulnerability

Flawed processing of ‘additional section’

ATTACK METHOD

- Attacker controls authoritative names server and a domain: attacker.com
- Attacker tricks user to resolve attacker.com (hacked site, mail, social media, hidden picture, ..)

ATTACK EXECUTION

- Client resolves attacker.com
- Name server replies with an [additional section] in DNS response, adding unrelated information for bank.com

```
;; ADDITIONAL SECTION:
www.bank.com.  99999 IN A 11.22.33.44
mail.bank.com. 99999 IN A 11.22.33.44
```

- Resolving server caches attacker.com and www.bank.com information

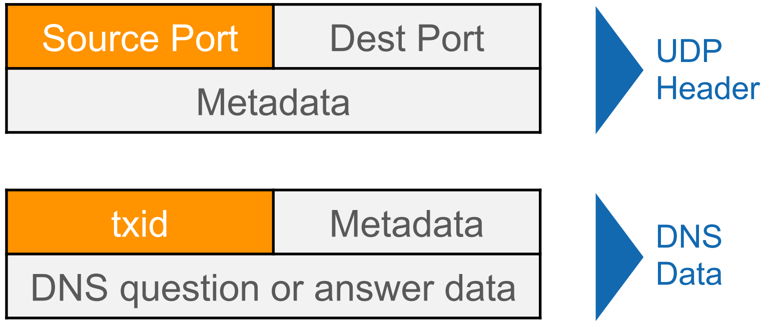
REMEDIATION

- This was an early vulnerability in the resolver: Accepting and caching information not related to the query
- All major DNS servers and libraries patched since ~ 1997

Cache Poisoning - Guessing Game

Challenges to inject incorrect information

DNS PACKET ON WIRE

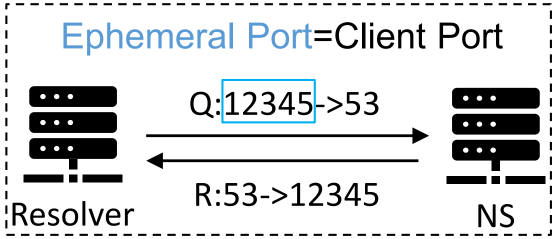


THREE POSSIBLE ANSWERS TO DNS REQUEST

1. “Here’s your answer”
2. “Go away”
3. “I don’t know, ask that name server over there” (**Delegation**)

ATTACKERS VIEW

- Only knowing the txid and source port prevent the attacker to insert his own information
- At best attacker can guess: port and txid entropy (at max): 2^{16} x 2^{16} = $65{,}536^2$ – **bad odds to win**
- Attacker needs to wait **until next race** if his response is **late** or **wrong** – the correct info is cached until TTL expires



In a perfect world the good guy (the real name server) has a 65,536 x 65,536 to 1 advantage over the attacker.
- HOWEVER, WE LIVE IN THE REAL WORLD!

Cache Poisoning - Guessing Game

Turning the odds

ATTACKER CAN FORCE A SERVER TO LOOK SOMETHING UP

- Client-server request & response round-trip takes time
- It takes attacker no time to immediately a send fake response

WHO SAID YOU CAN ONLY REPLY ONCE?

- Try lots of random txid – no need to wait for anything
  - *100 replies before good reply turn 1 : 65,000 to 1 : 650*

WHO SAID YOU CAN ONLY USE ONE DOMAIN NAME?

- Lookup www.bank.com a hundred times – 1st race likely lost
  - *99 suppressed by TTL*
- Lookup [1.100].www.bank.com – attacker gets 100 races
  - *TTL only stops race for one domain name*

ATTACKER WILL EVENTUALLY SPOOF 83.www.bank.com

- Then send nameserver redirect > Delegation
- Control nameserver for bank.com

KAMINSKY ATTACK

```
# (1) STARTER PISTOL
#     send query to nameserver
Select $RANDOM.www.bank.com

# (2) Send multiple replies with different TXID
#     and name server redirection data
200 fake replies with TXID 0-200 and NS redirect

# (3) If it works: OK
#     else: return to step 1
```

NAMESERVER REDIRECTION

```
;; AUTHORITY SECTION:
83.www.bank.com. 99999 IN NS www.bank.com 11.22.33.44
;; ADDITIONAL SECTION:
www.bank.com.    99999 IN A 11.22.33.44
```

Source: http://kurser.lobner.dk/dDist/DMK_BO2K8.pdf

SADDNS Attack
Nov 2020

Cache Poisoning: SADDNS

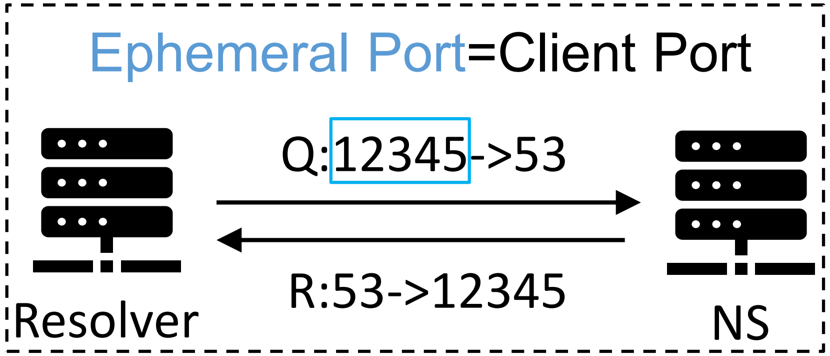
DNS Cache Poisoning Attack Reloaded

NOVEL APPROACH

When a DNS server issues a query, its source port effectively becomes open to the public

- Trigger a query on target server (source port becomes open to public)
- Scan port range with UDP to identify open source port:
  - Triggers nothing upon hitting the correct port (as the probe will be accepted by the OS but discarded at the application layer - src ip mismatch)
  - ICMP port unreachable message upon missing it

- Once the source port number is known, the attacker simply injects a large number of spoofed DNS replies bruteforcing the txid



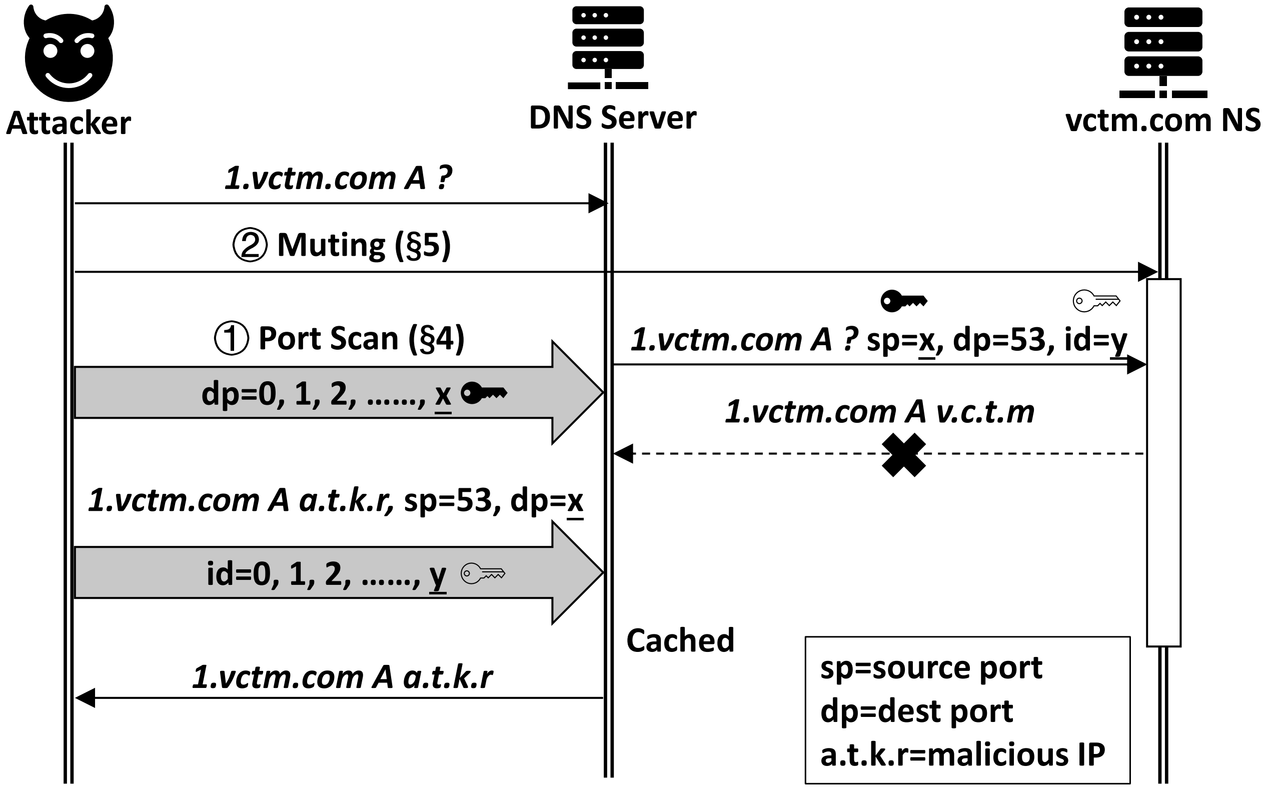
Source: https://www.saddns.net/

Cache Poisoning: SADDNS

DNS Cache Poisoning Attack Reloaded

ATTACK WORKFLOW

1. Trigger the DNS server to send a query *(source port becomes open to public)*
2. Mute victim NS to delay response (buy time for attacker)
3. Port scan DNS server *(dropped packed indicates open port)*
4. Send fake reply



TRICKS TO OVERCOME ICMP RATE LIMITS

- Use multiple source IPs (or IPv6)
- Infer by probing ICMP rate limit after scan with fake IPs
- Result: 60+ seconds to enumerate the entire port range consisting of 65536 ports.

Cache Poisoning: SADDNS

DNS Cache Poisoning Attack Reloaded

DEFENSES

- DNSSEC
- 0x20 encoding (mixed case encoding)
- Disable ICMP port unreachable
  (or DROP rather than REJECt at Firewall)
- Randomize ICMP global rate limit

PUBLIC RESOLVERS

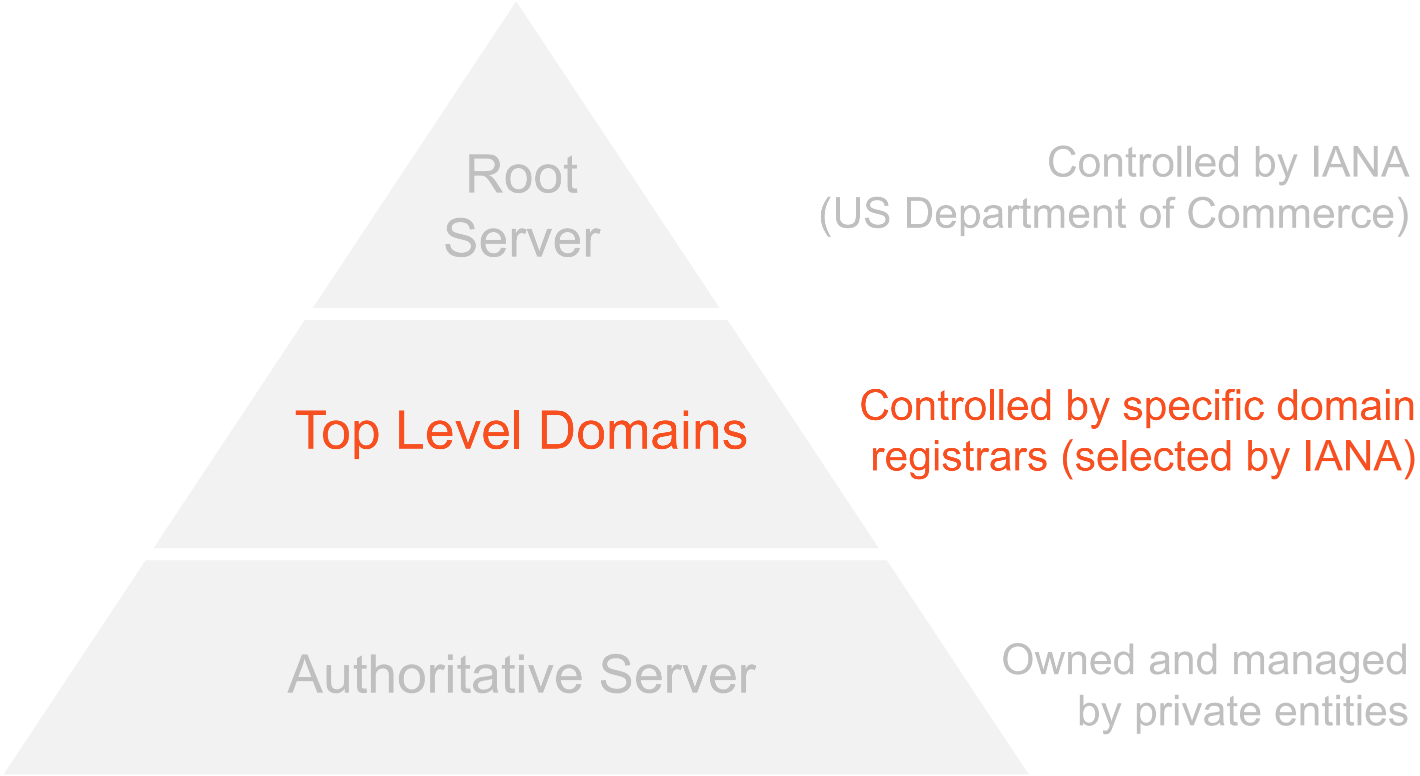
12 / 14 vulnerable

Google	8.8.8.8
Cloudflare	1.1.1.1
OpenDNS	208.67.222.222
Comodo	8.26.56.26
Dyn	216.146.35.35
Quad9	9.9.9.9
AdGuard	176.103.130.130
CleanBrowsing	185.228.168.168
Neustar	156.154.70.1
Yandex	77.88.8.1
Baidu DNS	180.76.76.76
114 DNS	114.114.114.114
Tencent DNS	119.29.29.29
Ali DNS	223.5.5.5

Attack Pattern
Compromised Configuration

Attack Domain Registrar

Provisioning wrong information



COMPROMISE DOMAIN REGISTRAR

Second level domains (SLD) are registered with one of the domain registrars of the TLD

- The DNS information is as secure as the **Web App**, **Registration Processes**, or the **Passwords** of the registrar and the domain owner

ATTACK

- Hack the Web App of the domain registrar
- Brute-force users password *(or get it from a data breach)*

THEN

- Change registration entries directly at the registrar
- Lock owner out of his account *(password resent mails wont work anymore)*

Attack Domain Registrar

Provisioning wrong information

DEFENSE

- Monitor your account and name server entries of your domains for critical services
- Use strong passwords and multi factor authentication

Peru Domains Registrar hacked and domain panel credentials leaked (2012)

PERU DOMAIN REGISTRAR HACKED & 207,116 DOMAIN CREDENTIALS STOLEN - ANONYMOUS GROUP

POSTED NOV 05 2012 | Stephen Coty

One of the biggest Peru domain registrar companies (punto.pe) was hacked by Lulzsecperu, and a complete database of 207,116 websites has been leaked on the Internet. The leaked database includes domain panel usernames, encrypted passwords and company descriptions. Hacked domains include bank, institute, computer security company, corporate, college, government and personal websites. http://alrt.co/VNC1zc

Takeaway: Though no malicious purpose was seen and the hack was only done to prove that the security of Peru should be corrected, the outcome was a result in vulnerabilities that were either not patched or overseen by a busy/negligent IT administrator. Automated security monitoring and review from a second set of eyes helps greatly in such circumstances.

DNS hijack and extremely well-executed spoofed sites fool bank customers

How Hackers Hijacked a Bank's Entire Online Operation (2017)

Earlier this month, the security firm Kaspersky detailed the wholesale takeover
attack itself was a quintessential DNS hijack where the attackers took over severa
of five hours, customers were directed by NIC.br (the company that manages the bank's DNS service and, incidentally, the domain registrar for the Brazilian top-level domain, .br) to spoofed versions of the bank's legitimate sites. The spoofed sites were reportedly near perfect down to having their own valid SSL issued in the name of the bank.

https://thehackernews.com/2012/10/peru-domains-registrar-hacked-and.html
https://www.wired.com/2017/04/hackers-hijacked-banks-entire-online-operation

Attack Network & Local Configuration

Insecure provisioning of DNS setting

ATTACK PATTERN

- Manipulate DNS configuration settings on internal network or local host
- Have target point to attackers name server

WAN NETWORK

- Scan ISP networks, identify vulnerable routers or weak / default passwords
- Attack poorly protected client router of Internet Service Providers (ISP)

LAN NETWORK

- Attack client router or DHCP server directly
- Attack DHCP exchange in local network:
  Cache poisoning against DHCP: attacker replies faster than DHCP server ..

LOCAL HOST

- Manipulate DNS local hosts settings on compromised machine:
  Malware changes local DNS configuration

Attack Network - WAN

WAN level domain hijacking

- Poor security of ISPs can lead to mass compromise of customer routers
- Attacker controls all client traffic after changing the name server in the routers
- Hard to detect for end-users (everything still works, no local machine compromised)

2014

Many home routers supplied by ISPs can be compromised en masse, researchers say

By Lucian Constantin
Romania Correspondent, IDG News Service | AUG 10, 2014 6:45 AM PT

2016

30 New Mirai Worm Knocks 900K Germans Offline

NOV 16

More than 900,000 customers of German ISP **Deutsche Telekom** (DT) were knocked offline this week after their Internet routers got infected by a new variant of a computer worm known as **Mirai.** The malware wriggled inside the routers via a newly discovered vulnerability in a feature that allows ISPs to remotely upgrade the firmware on the devices. But the new Mirai malware turns that feature off once it infests a device, complicating DT's cleanup and restoration efforts.

Researcher warn of routers publicly exposing the ISP management protocol TR-069 or CWMP (customer-premises equipment wide area network management protocol) (2014)

Mirai botnet compromises 900k+ routers of German ISP, abusing TR-069 (2017)

https://www.pcworld.com/article/2463480/many-home-routers-supplied-by-isps-can-be-compromised-en-masse-researchers-say.html
https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/

Attack Local Machine
Local Network Configuration

ATTACK PATTERN
- The local hosts file for static mapping of names to IPs
- Entries in hosts file usually precede DNS resolution

MALWARE DISABLES PROTECTION
- Malware disables access to anti-virus, security updates, blacklists by entries in hosts file that point to nowhere or localhost

Local host file entry to disable antivirus updates

LOCAL HOSTS FILE

```
# Location
# Windows   /etc/hosts
# Linux:    C:\Windows\System32\Drivers\Etc\

# Disable AV
antivirus.com           127.0.0.1
update.mcafee.com       127.0.0.1
...
```

Source: https://techzoom.net/whitepaper/cyber-crime-threat-intelligence-turkey/

Attack Local Machine

DNS Changer Botnet

Botnet changes DNS settings on infected hosts.
Name server configuration now points to name server of attacker.

IMPACT: 4 MILLION INFECTED HOSTS

- Ad manipulation (Google Ads)
- Phishing (credit cards, online banking)
- Selling software (fake iTunes shops)

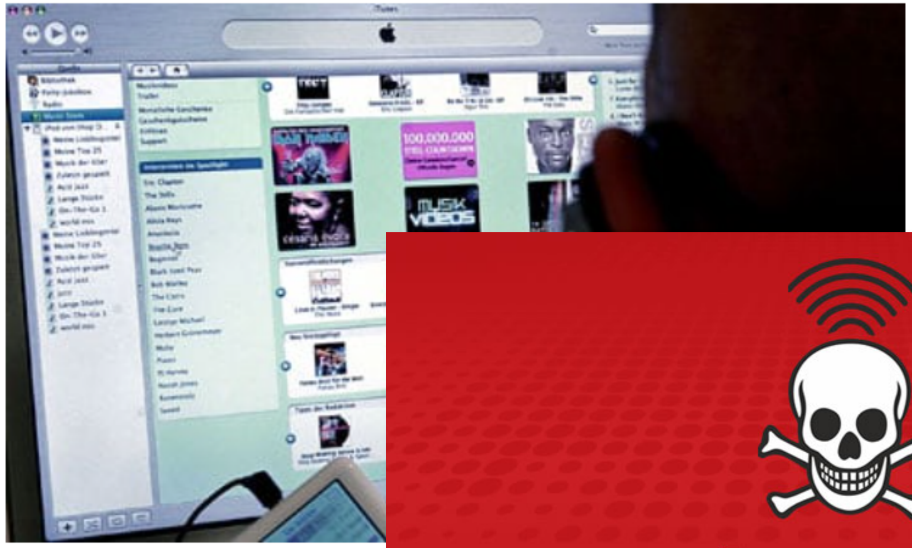
OPERATION GHOST CLICK / JULY 9TH, 2011

- FBI takes over the malicious name servers
- Six cyber criminals were taken into custody

REMEDIATION

- Switching off the malicious DNS servers at large i difficult
- March 8th, 2012
- Servers are still used by at least 250.000 hosts

'DNSChanger' misdirected searches for Apple's iTunes and US Internal Revenue Service from 2007 and earned criminals $14m, says US law enforcement



Apple iTunes: the DNSChanger malware woul
Oliver Stratmann/AFP/Getty Images

https://www.theguardian.com/technology/2011/nov/10/ghost-click-botnet-infected-computers-millions
https://thehackernews.com/2018/10/ghostdns-botnet-router-hacking.html

Lessons Learned

Cache Poisoning: Ongoing Arms Race

Attackers are creative, supported by implementation flaws

SECURITY LESSONS (BEYOND DNS)

SOURCE PORT

GUESSING THE SOURCE PORT MADE EASY

- Resolvers used a single open port (typically 53) or predictable source ports (known sequence) – *until ~ 2008*
- Port remapping in NAT or gateway devices reduce port randomness

TRANSACTION ID

INSUFFICIENT RANDOMNESS AND ENTROPY

- txid incremented for every request – *until ~ 2000*
- Entropy only 16 bit – *by design*
- Mixed case DNS queries add entropy [1] ~ 2008

DATA VALIDATION

BAILIWICK CONSTRAINT

- Domain nasty.com can add delegations for bank.com - *until ~ 1997*

BIRTHDAY PARADOX

PROCESSING OF MULTIPLE REPLIES

- Multiple outstanding requests for the same resource record

[1] http://courses.isi.jhu.edu/netsec/papers/increased_dns_resistance.pdf

Name Server Roles

Recursive name servers that resolve queries for anybody are a security problem:

- Can be abused to launch powerful DDoS attacks from anywhere

	AUTHORITATIVE SERVER	CACHE / RECURSIVE RESOLVER
VISIBILITY	▪ Respond to queries from any source	▪ Respond to “local” network only
TYPES OF QUERIES	▪ Non recursive queries	▪ Recursive queries
RECORDS	▪ Only with data it is authoritative about	▪ Should attempt to resolve any legitimate request

DNSSEC

Domain Name System Security Extensions (DNSSEC)

Add security, while maintaining backward compatibility

DNSSEC IS A SET OF EXTENSIONS TO DNS

DNSSEC VERIFICATION PROVIDED	**DNSSEC** NOT PROVIDED
▪ Origin authentication ▪ Authenticated denial of existence ▪ Integrity	▪ DNS availability ▪ Data confidentiality

DNSSEC Key Features

- DNSSEC zone data is digitally signed using a private key for that zone
- DNSSEC can protect any data published in the DNS

A DNS server receiving DNSSEC signed zone data can verify the origin and integrity of the data by checking the signature using the public key for that zone

https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en

DNSSEC – Signed Zones

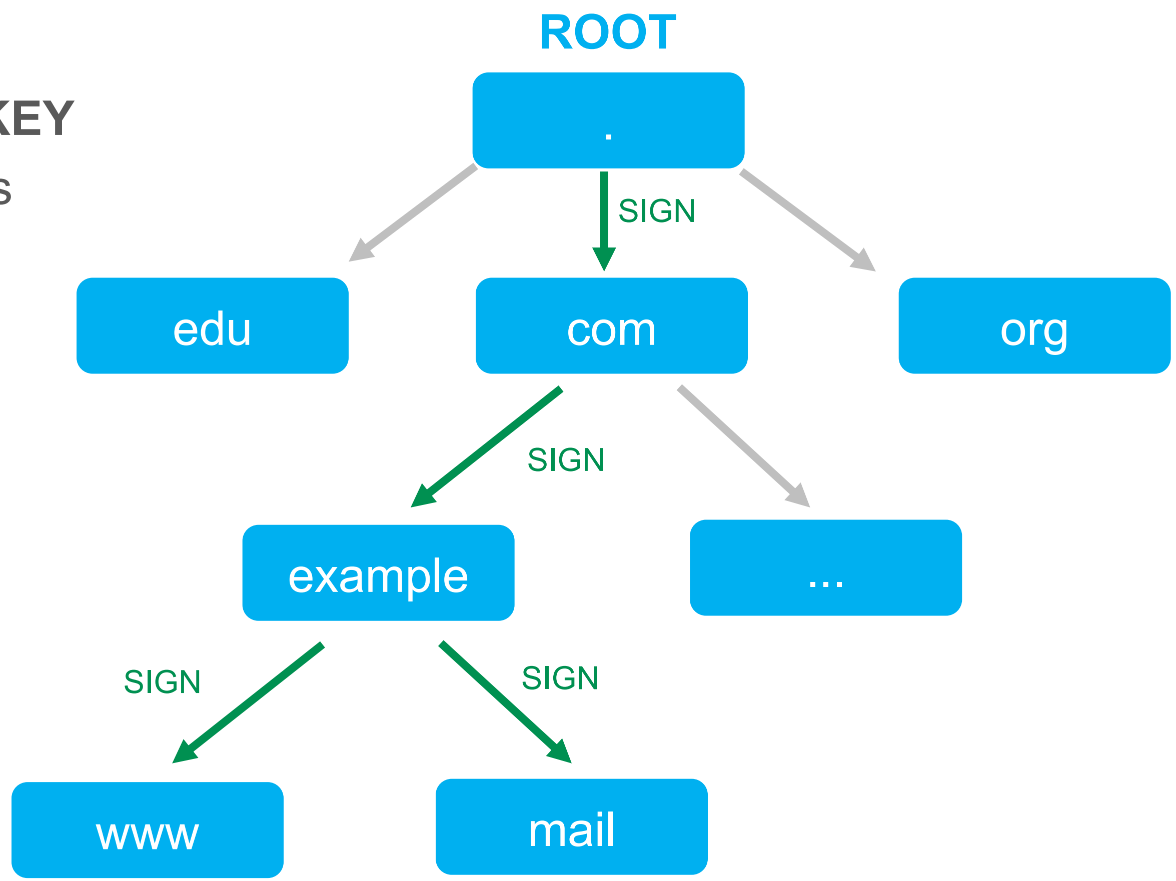
Basic idea is a hierarchy of signed zones

EACH DNS ZONE SIGNS ITS DATA USING A PRIVATE KEY

- Use public-key signature to authenticate DNS messages
- **Parent signs children's public keys**
- Resolver only needs to know the root public key to authenticate DNS messages

TO MAKE DNSSEC WORK

- **Registrants** (responsible for publishing DNS information), must ensure their DNS data is DNSSEC-signed.
- **Network Operators** need to enable DNSSEC validation on their resolvers that handle DNS lookups for users.



A resolver has a list of trust anchors, which are public keys for different zones that the resolver trusts implicitly.

Source: https://www.icann.org/en/system/files/files/dnssec-help-secure-info-10jun20-en.pdf

DNSSEC Protection Process

Add security, while maintaining backward compatibility

EACH DNS ZONE SIGNS ITS DATA USING A PRIVATE KEY

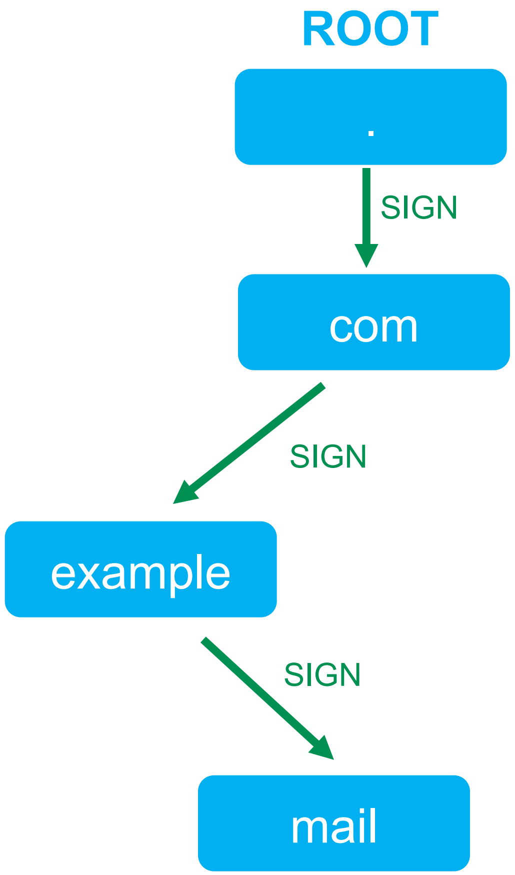
- Recommend signing done offline in advance

A QUERY FOR A PARTICULAR RECORD RETURNS

- The requested resource record set
- A signature (SIG) of the requested resource record set

THE RESOLVER AUTHENTICATES RESPONSE

- Verify with trusted public key(s)
- Validation done with pre-configured key or keys learned via a sequence of queries to the DNS hierarchy
- At least one trusted public key is pre-configured



DNSSEC Resource Records

DNSSEC adds new types of DNS records

RECORD TYPE	DESCRIPTION	USAGE
`RRSIG`	RESOURCE RECORD SIGNATURE	DNSSEC signature for a record set. Resolvers verify the signature with a public key, stored in a DNSKEY-record.
`DNSKEY`	PUBLIC KEY RECORD	Contains the public key that a resolver uses to verify DNSSEC signatures in RRSIG-records
`DS`	DELEGATION SIGNER RECORD	Holds the name of a delegated zone. DS record is placed in the parent zone along with the delegating NS-records. References a DNSKEY-record in the sub-delegated zone.
`NSEC`	NEXT SECURE RECORD	Contains a link to the next record name in the zone and lists the record types that exist for the record's name. DNS Resolvers use NSEC records to verify the non-existence of a record name and type as part of DNSSEC validation.

CLIENT	SERVER
Indicates DNSSEC support	Include RRSIG signature if DNSSEC is supported

DNSSEC Slow Adoption

DNSSEC extension introduced around 2000

HISTORY

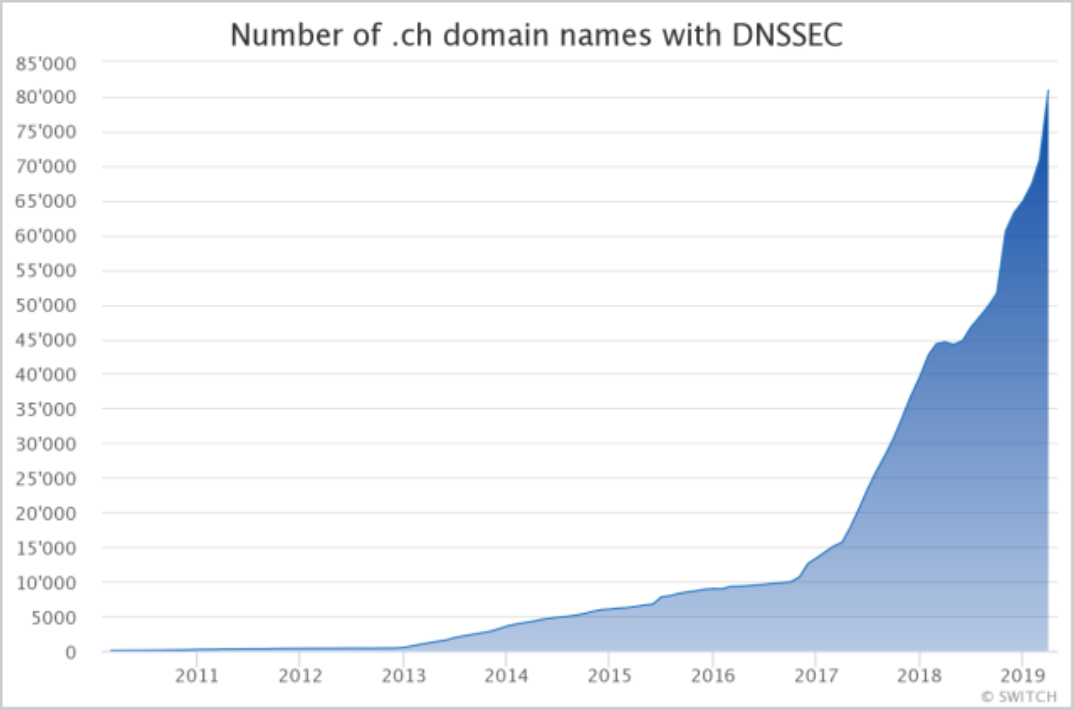
- **1993**: first discussions and requirement analysis in IETF
- **1997/1999**: first RFCs
- **2005**: complete new approach: RFCs 4033 – 4035
- **2010**: DNSSEC supported by all root servers
- **2013**: Google Public DNS enables DNSSEC validation by default

GLOBAL ADOPTION (2017)

Only a small fraction of domains is signed

- 0.7% for .com domains
- 1% for .org domains
- 1.85% for Top Alexa 10K domains

DNSSEC ADOPTION in SWITZERLAND



Number of signed domainnames is still very low at around 3-4%

Source: https://securityblog.switch.ch/2019/04/02/dnssecinswitzerland2019/

DNSSEC
Mixed Results

DNSSEC ADVANTAGES	**DNSSEC** DISADVANTAGES
▪ Origin authentication ▪ Integrity protection ▪ Stops DNS spoofing attacks	▪ High Complexity ▪ Performance ▪ No confidentiality protection ▪ Adversary can gradually learn all host names (“zone walking”) ▪ Large response messages *(DNS amplification, TCP)* ▪ Still no browser support ▪ Slow adoption
▪ DNSSEC now deployed at key zones including net, com, gov, and edu	▪ Against the initial design principles of DNS: autonomy of individual zones

DNS over HTTPS (DoH) or TLS (DoT)

ADDING CONFIDENTIALITY TO DNS

Two protocols for adding confidentiality to DNS

PROBLEM

- DNS messages are not protected from eavesdropping (even with DNSSEC)
- DNS request are an easy way of tracking users (by the ISP or intelligence services)

DNS over TLS (DoT)

- DoT uses service specific port (853)
- Port might be filtered by firewall / attacker

DoT
DNS
TLS
TCP
IP

DNS over HTTPS (DoH)

- DoH uses standard HTTPS port (443)
- Usually no filtering, easy integration

DoH
DNS
HTTP
TLS
TCP
IP

Source: https://www.cloudflare.com/learning/dns/dns-over-tls/

CHALLENGES

Two protocols for adding confidentiality to DNS

STATE

- Not very widespread
  Browsers, Operating Systems, and DNS resolvers start to support DoH / DoT around end of 2020
- Possible solution: Using public (recursive) name servers
  8.8.8.8 (Google), 1.1.1.1 (Cloudflare)

NEW PROBLEM CREATED

- Trust in DNS server operator required (even more data for Google?)
- No “local” DNS entries (e.g. company Intranet)
- No or limited DNS blocking at the ISP / provider
- The 2019 DDoS worm Godula used DoH to mask connections to its command-and-control server

Monitoring and censorship are feasible even when DNS is encrypted (statistical analysis of encrypted traffic)

Source: https://en.wikipedia.org/wiki/DNS_over_HTTPS

Conclusion

Take Home Message

DNS HAS SUFFERED A SORT OF FEATURE CREEP, PICKING UP MORE AND MORE RESPONSIBILITIES.

- Do not underestimate complexity of protocols paired with creative attackers
- Ensure large enough randomness / entropy for critical fields
- Threat model different use and abuse cases upon design
- Consider impact of input validation, rate limiting, max outstanding/open connections

Terminology

RESOLVER	A DNS client that sends DNS messages to obtain information about the requested domain name space.
RECURSION	The action taken when a DNS server is asked to query on behalf of a DNS resolver.
AUTHORITATIVE SERVER	A DNS server that responds to query messages with information stored in RRs for a domain name space stored on the server.
RECURSIVE RESOLVER	A DNS server that recursively queries for the information asked in the DNS query.
FQDN	A Fully Qualified Domain Name is the absolute name of a device within the distributed DNS database.
RR	A Resource Record is a format used in DNS messages that is composed of the following fields: NAME, TYPE, CLASS, TTL, RDLENGTH, and RDATA.
ZONE	A database that contains information about the domain name space stored on an authoritative server.