DNS and DNSSec

By: Syed Usman, Jonas Laya, Paul Sison

Overview

- What is DNS?
- Vulnerabilities and Attacks
- DNSSec as a solution

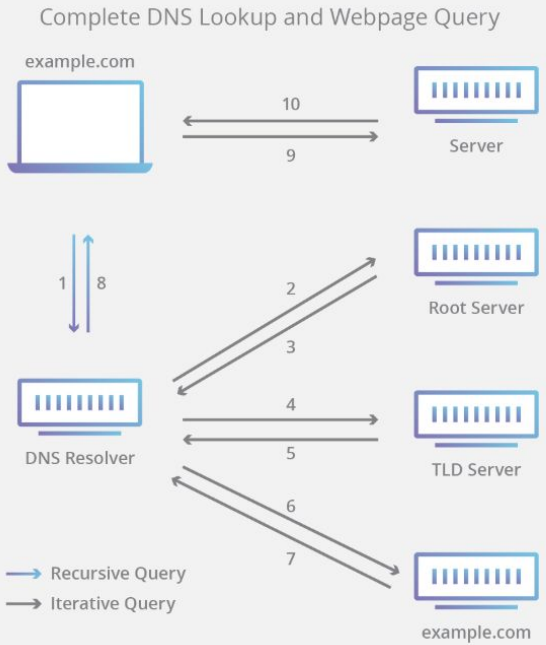
What is DNS?

DNS

“Phonebook of the Internet”

- Domain Name System
- Translates domain names to IP addresses
- Motivation
  - Eliminates memorizing IP addresses
- Application Layer Protocol
- Operates on UDP port 53
  - Fast and low overhead

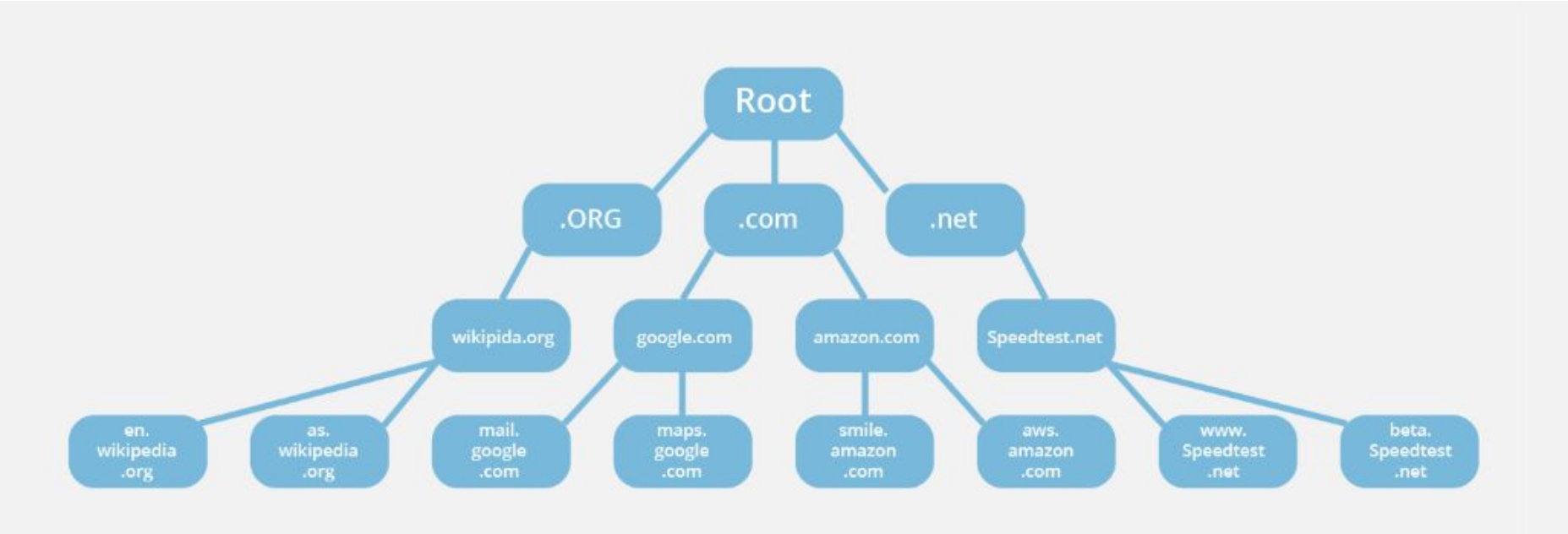
DNS Lookup



https://www.cloudflare.com/learning/dns/what-is-dns/

- DNS Resolver
  - Receives DNS queries from applications such as browsers
- Root Server
  - Provides TLD address
- Top-Level-Domain Server
  - Provides nameserver address
- Authoritative Name Server
  - Provides hostname's IP address

DNS Hierarchy



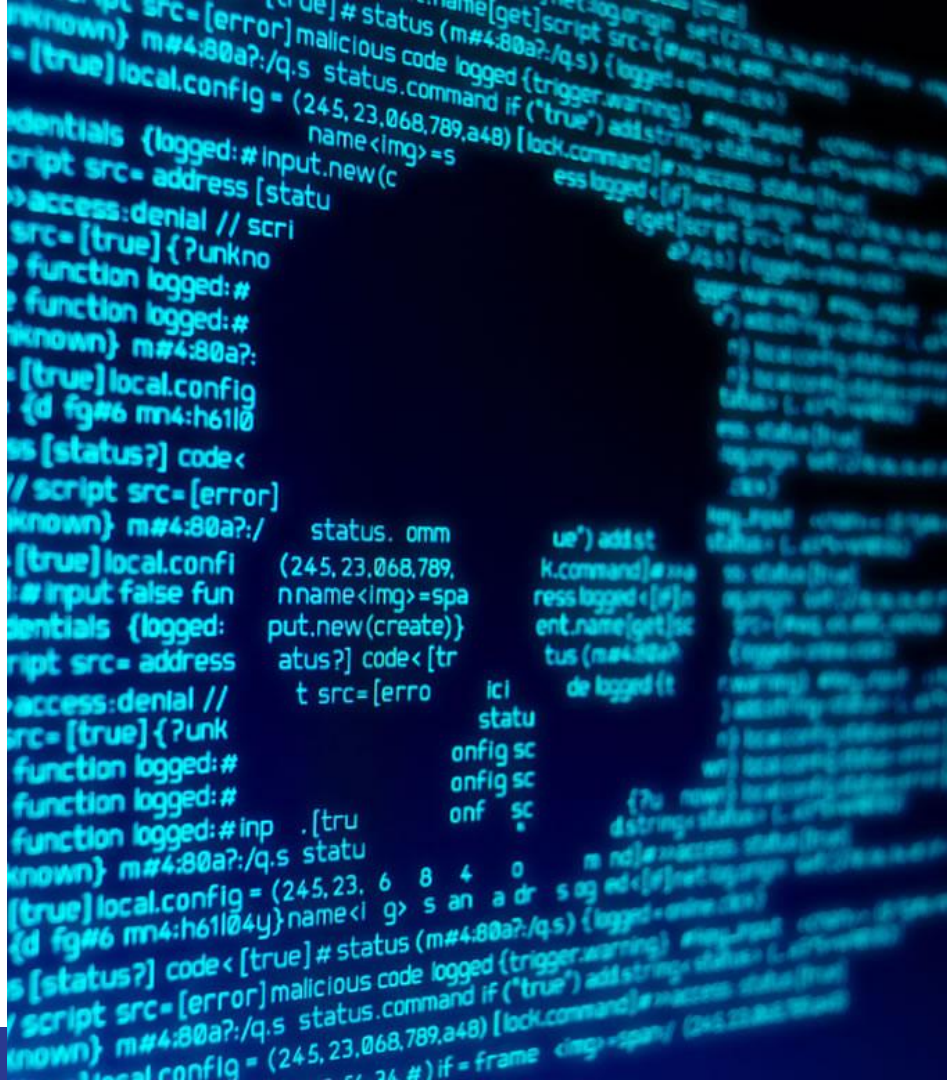
https://www.cloudflare.com/learning/dns/glossary/dns-root-server/

Vulnerabilities

Attacks

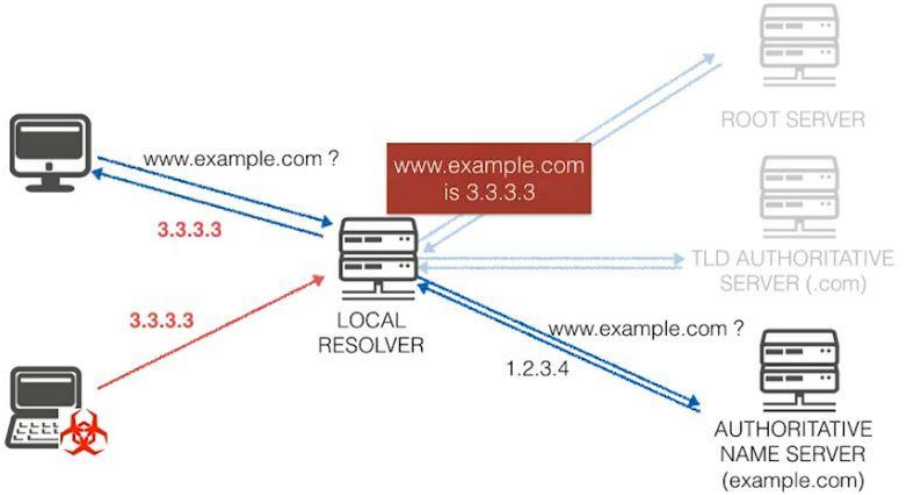
Vulnerabilities

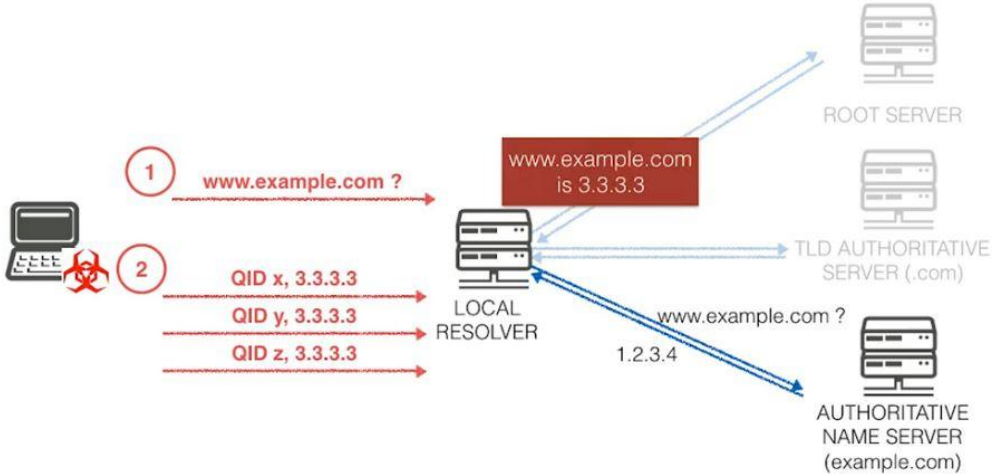
- Use of unsigned, unencrypted UDP packets
  - No source authentication
  - No data integrity check
- Use of cache for reduced access time
  - Cache inconsistency
  - Staleness of data
- Stored data (Resource Records) on name servers



Cache Poisoning

- Exploit on usage of UDP and a cache
- Method 1: Packet Interception
  - Man-in-the-Middle attack
- Method 2: ID Guessing and Query Prediction
  - Old servers used sequential transaction IDs
- 1996 - InterNIC
- 2008 - Kaminsky bug
  - Replaces NS Authority record in cache for target domain

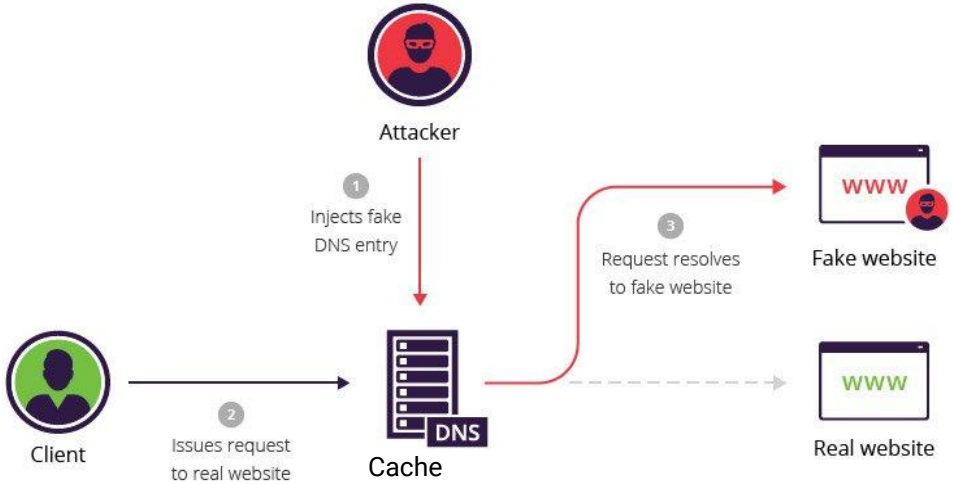




https://youtu.be/lVifa7QSQDY

Cache Poisoning

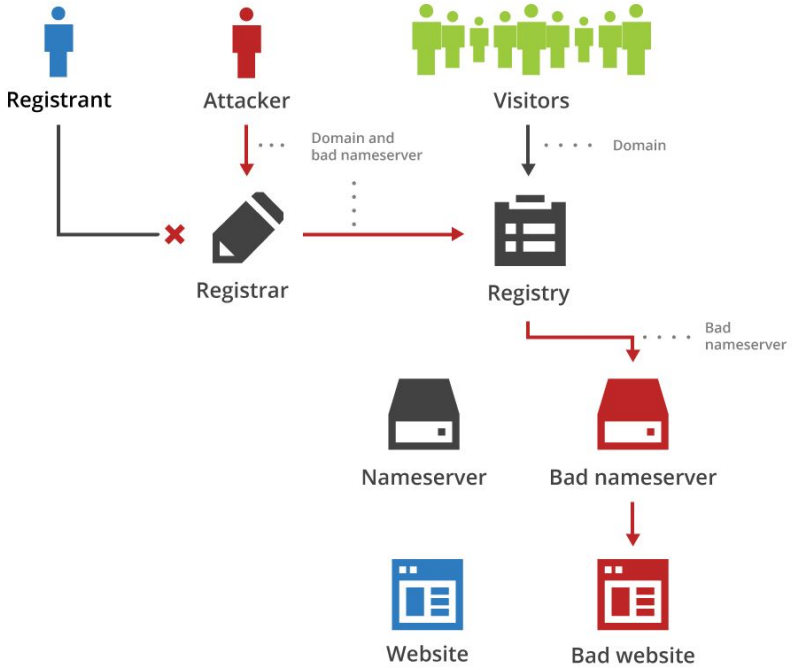
- Exploit on usage of UDP and a cache
- Method 1: Packet Interception
  - Man-in-the-Middle attack
- Method 2: ID Guessing and Query Prediction
  - Old servers used sequential transaction IDs
- 1996 - InterNIC
- 2008 - Kaminsky bug
  - Replaces NS Authority record in cache for target domain



https://www.imperva.com/learn/application-security/dnssec/

Domain Hijacking

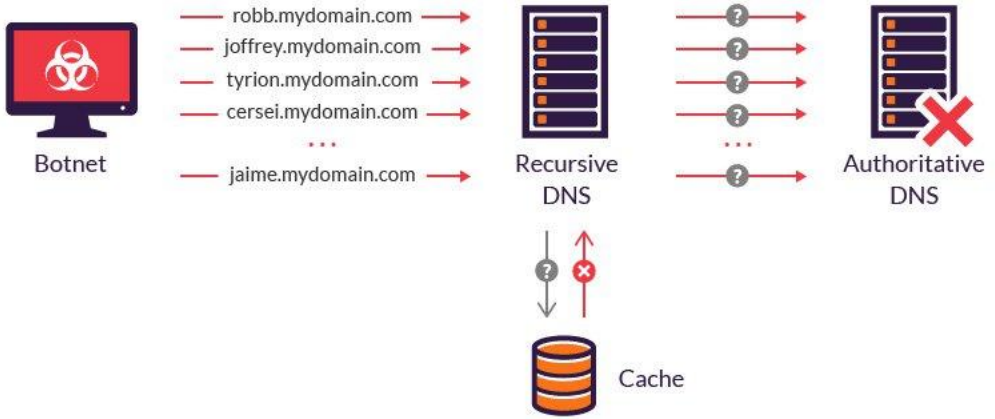
- Attackers take control of the domain registration
- Domain information changed to point to a malicious nameserver
- 2008 - icann.org & iana.org
  - Social engineering
- 2016 - Brazilian banks
  - 6 hours, $27B of assets
- Unpaid registrar bill



https://blog.cloudflare.com/introducing-cloudflare-registrar/

DNS Flood

- DoS attack to deny legitimate requests
  - UDP easy to forge, no handshake required
  - Exhaust all available UDP sockets
- 2013 - Spamhaus
- 2015 - .tr ccTLD name servers
  - Isolated Turkey from the World
- Poorly-formatted DNS requests
  - 14% of queries on root servers



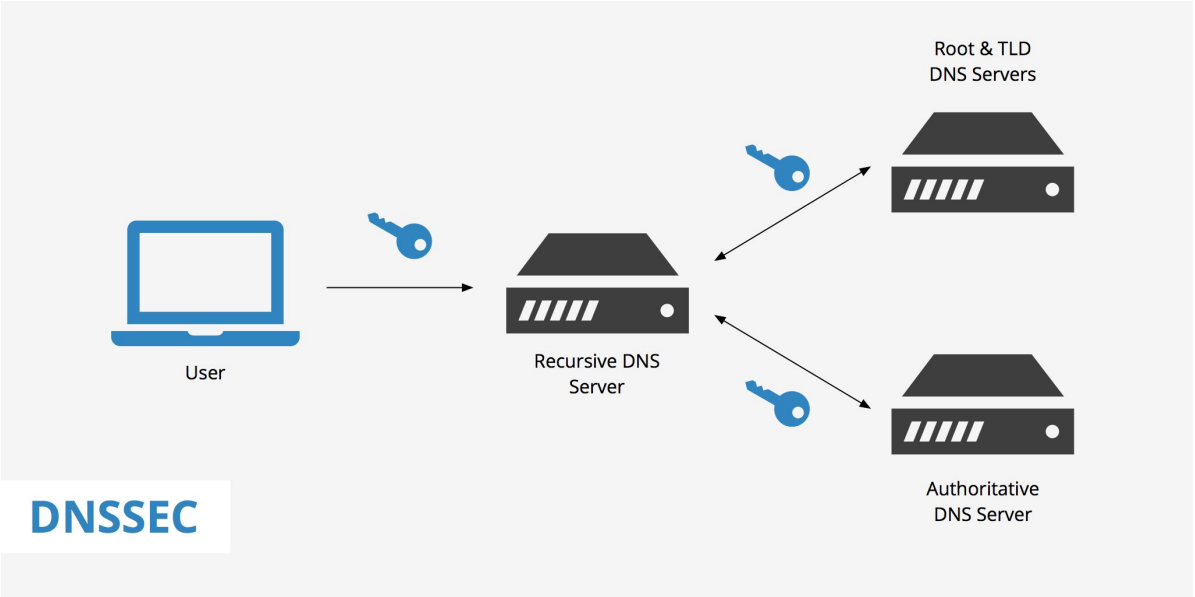
https://www.imperva.com/learn/application-security/dns-flood/

DNSSec

- Provides security for the DNS protocol
- Created in 2005 and made fully usable in 2010 (ICANN)
- Ensures
  - Origin Authentication
  - Data Integrity
  - Authenticated Denial of Existence

How it Works ?

- Asymmetric Key Cryptography
- Hash Function



How it Works ?

- Recursive server has root server’s public key.
- Recursive server sends iterative request to root server.
- Root server responds back with
  - TLD server details
  - TLD server public key encrypted by it’s private key
  - Root servers public key record encrypted by it’s private key
- Recursive server uses root servers public key to
  - Decrypt these encrypted files
  - Gets the public key for the TLD server from decrypted file
  - Compare its public key with the one the root server sent
- The same process continues for TLD & Authoritative server.

DNSSec Vulnerabilities

- Increase the query response time
- Root public key injection attack would compromise the chain of trust
- DNSSec requires time synchronisation, if attacker can cause disruption in the synchronisation then DNSSec fails to work properly

Questions:

1. DNS is a protocol on which OSI layer?
2. Can the Internet survive without DNS?
3. How important is DNSSec ?

References

Issues in DNS Security. Online. https://cdn.ttgtmedia.com/rms/pdf/DNS%20Security_Ch%202.pdf

Ariyapperuma & Mitchell. Security Vulnerabilities in DNS and DNSSec. Online. http://web.mit.edu/6.033/www/papers/dnssec.pdf

What is DNS? How DNS Works. Online. https://www.cloudflare.com/learning/dns/what-is-dns/

Domain Name System. Online. https://en.wikipedia.org/wiki/Domain_Name_System

DNS Security - Cache Poisoning. Online. https://www.youtube.com/watch?v=lVifa7QSQDY

Atkins. Threat Analysis of the Domain Name System. 2004. Online. https://tools.ietf.org/html/rfc3833

DNS Flood. Online. https://www.imperva.com/learn/application-security/dns-flood/

DNSSec https://www.keycdn.com/support/dnssec