DNS TTL Values as Potent Allies of DDoS Attackers:

A Fact Overlooked by Some Major US and EU Banks

N. Vlajic, CSE Department, York University

DNS - Introduction

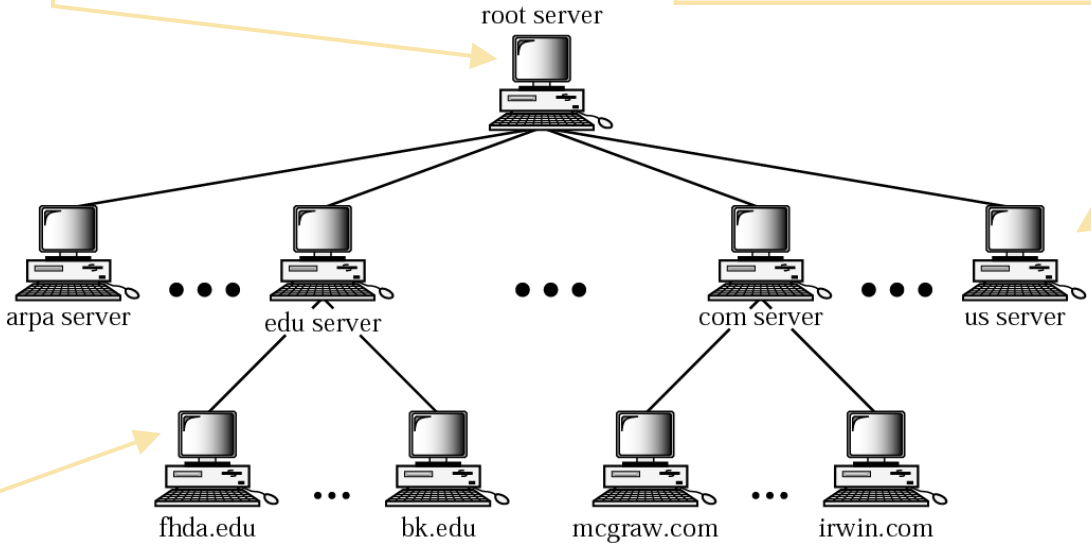
Domain Name System (DNS) – [distributed database + application layer protocol] that are essential to functioning of Internet

- performs '*symbolic name* ↔ *IP address*' translation
- Distributed DNS Database – implemented as a hierarchy of many DNS servers
- DNS Protocol – allows querying of DNS servers by other DNS servers and regular (end) hosts
  - runs over UDP (or TCP), with servers on port 53
  - generally not accessed directly by end users – DNS resolution takes place transparently in application programs such as web browsers, email tools

DNS - Database Topology

Root DNS Servers
– 13 addresses, 117 servers –
do not store any info, but keep reference to TLD servers

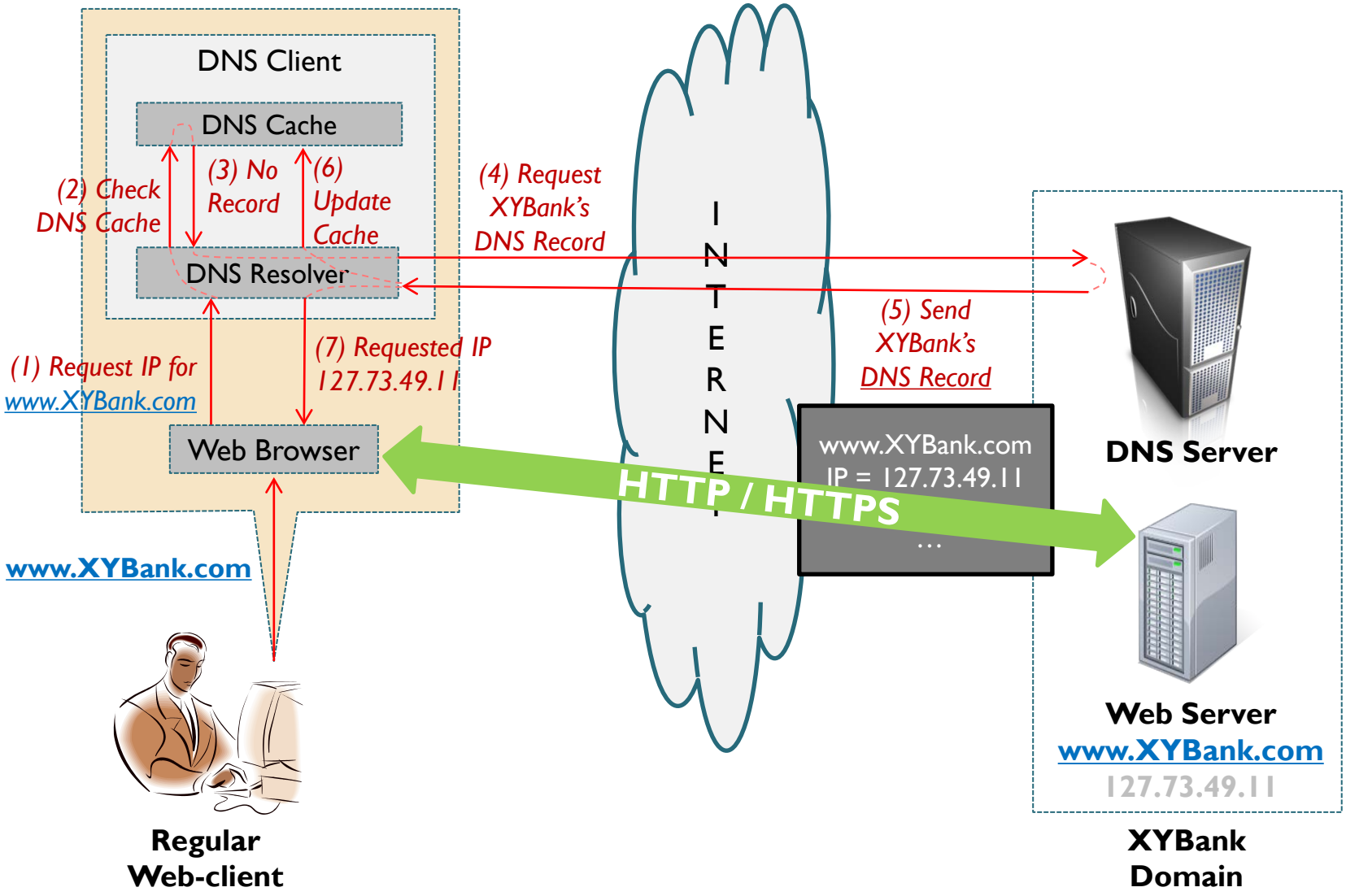
Top-Level Domain DNS Servers – responsible for domains such as: com, org, net, edu, gov, … and country level domains: uk, fr, ca, …



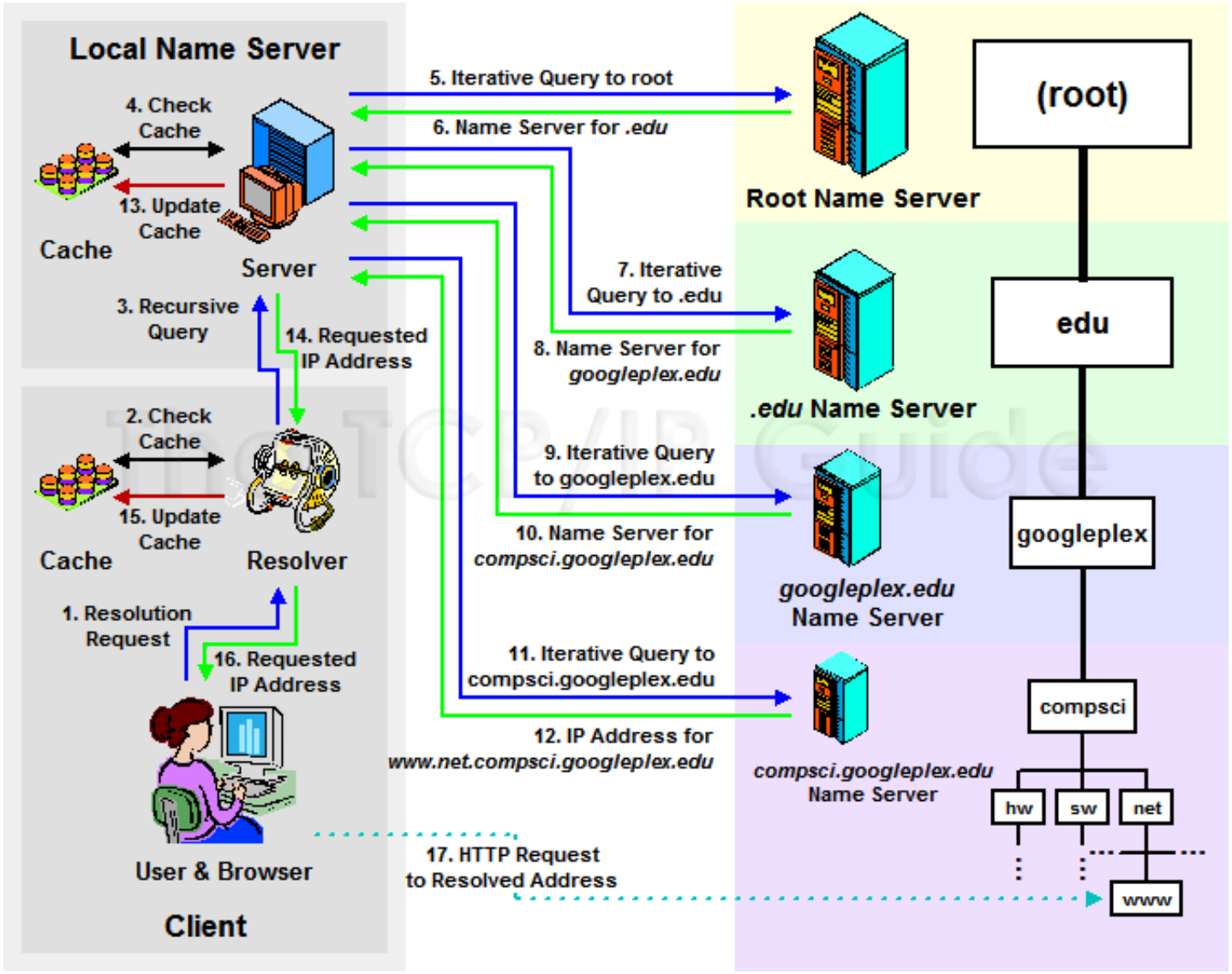
Authoritative DNS Servers – organization's DNS servers, provide hostname to IP mappings for all organization's publicly accessible hosts

Local DNS Servers – do NOT belong to hierarchy, yet crucial to DNS architecture. Each ISP, company, university, … has one. Local DNS servers receive queries from hosts and (possibly) forward them into DNS.

DNS System – Operation (1)



DNS System – Operation (2)



DNS System - Caching

Goals of DNS Caching – reduce the load on high-level DNS name servers and resolve queries more efficiently

- performed by clients and lower-level DNS servers
- **Time-to-Live (TTL) Time** – determines how long a DNS Record remains in a DNS Cache

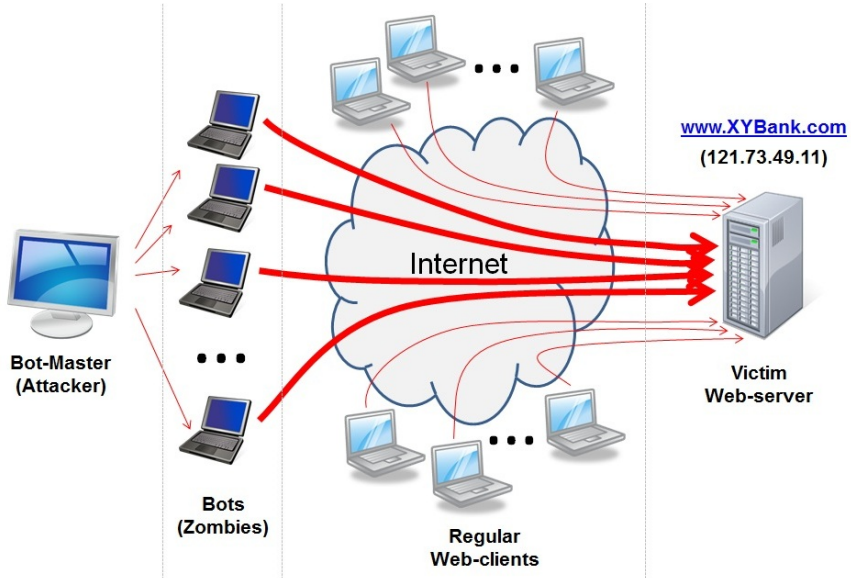
  - ✓ DNS requests likely served directly from clients' Caches ⇒ faster web-page download
  - ✓ fewer requests forwarded to higher-level DNS servers

  - ✗ infrequent Cache updates may cause problems in case of host failure followed by IP address migration

DDoS - Introduction

Distributed Denial of Service (DDoS) – concentrated effort to saturate the victim machine (web-server) with a large volume of traffic and/or processing

- server unable to provide service to regular users
- executed by a botnet – collection of compromised computers (bots) controlled by bot-master



DDoS – Long & Short Term Goals

DDoS Short-Term Goals – 'cut off' the server from as many regular users as possible

DDoS Long-Term Goals – tarnish victim's reputation and cause major financial loss

Session	The User and Business Impact of Server Delays, Additional Bytes, and HTTP Chunking in Web Search
Presenters	Eric Schurman (Microsoft), Jake Brutlag (Google)

...The%20User%20and%20Business%20Impact%20of%20Server%20Delays,...HTTP%20Chunking%20in%20Web%20Search%20Presentation.pptx

...ated populations changed one variable and measured

...lay: 1 second slowdown = 2.8% revenue loss; 2 second ...ue loss.

...on user satisfaction persists long after delays removed

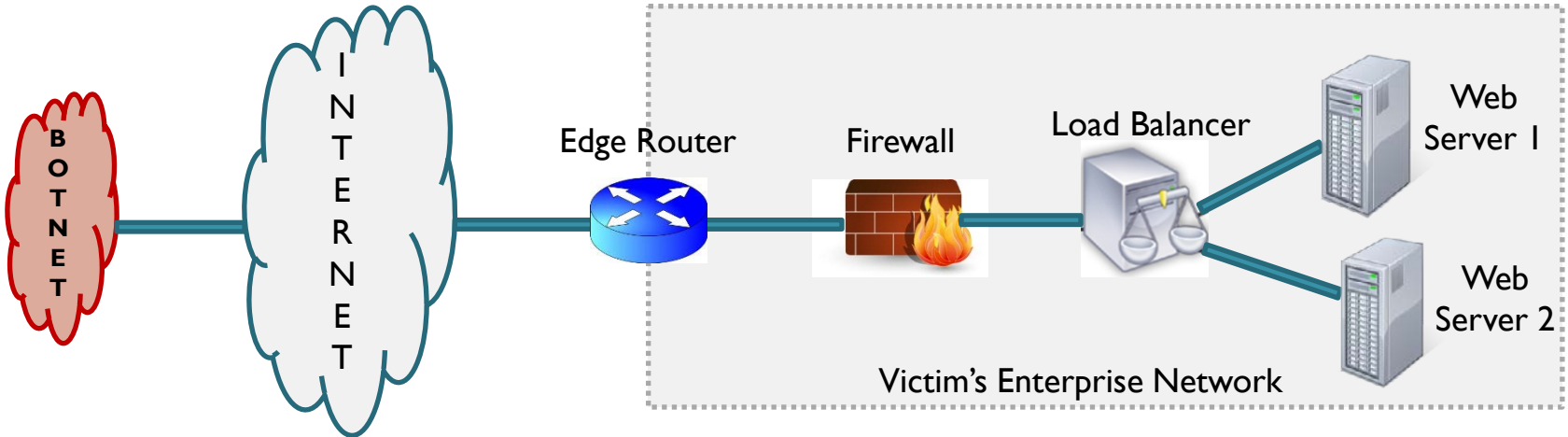
A report released by Forrester Consulting today, "The Impact of Poor Web Site Performance in Financial Services," finds that, unsurprisingly, bank customers' expectations for website performance are high, with 75% of online financial services consumers expecting 99% or higher web site availability. The findings of the study, which was sponsored by Akamai, also indicate that website performance is second only to security in user expectations; 36% of consumers who bank online and 42% of consumers who trade online consider 100% availability important.

More than half of online banking users (56%) expect web pages to load in two seconds or less, which is significantly more than the 47% of consumers who just shop online. Website performance ranks above even functions like single sign-on or ease of use. The study also found that 64% of online banking and brokerage customers have had dissatisfying experiences online.

DDoS - Defences

Places of DDoS Defence Implementation – almost exclusively at/near (victim) network

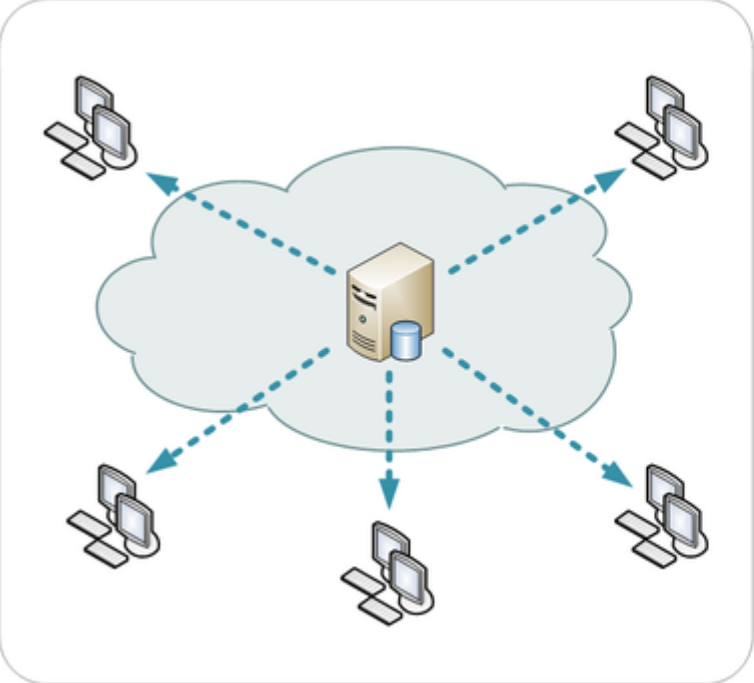
- Edge Router – perform filtering of blacklisted IP addresses
- Firewall – allow 'in' only trusted traffic/protocols + perform protocol inspection
- Load Balancer – distribute web-server (symbolic name) over multiple IP addresses
- Geographically Distributed Web-Server Replicas – servers do not share the common access path

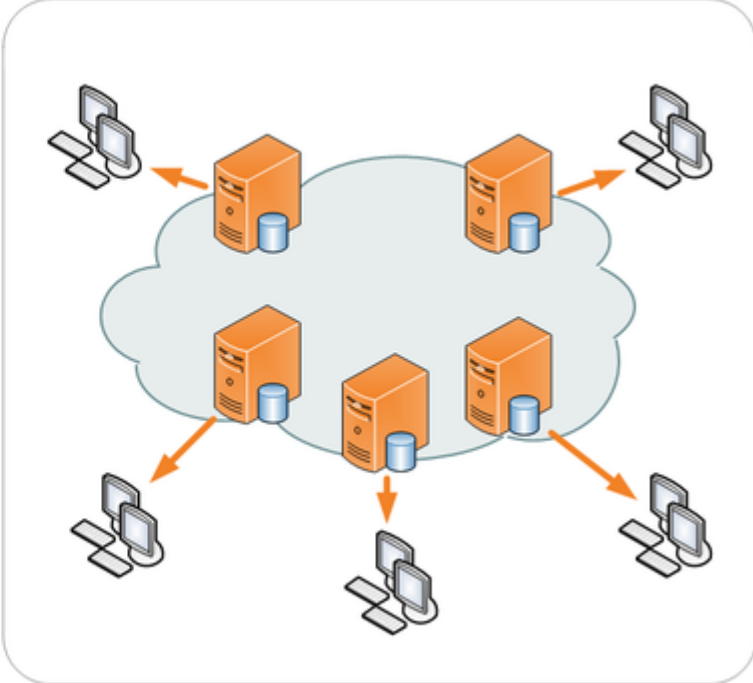


DDoS - Defences (cont.)

Example of Geographically Distributed Web Server Replicas:
Content Distribution Networks (CDN)

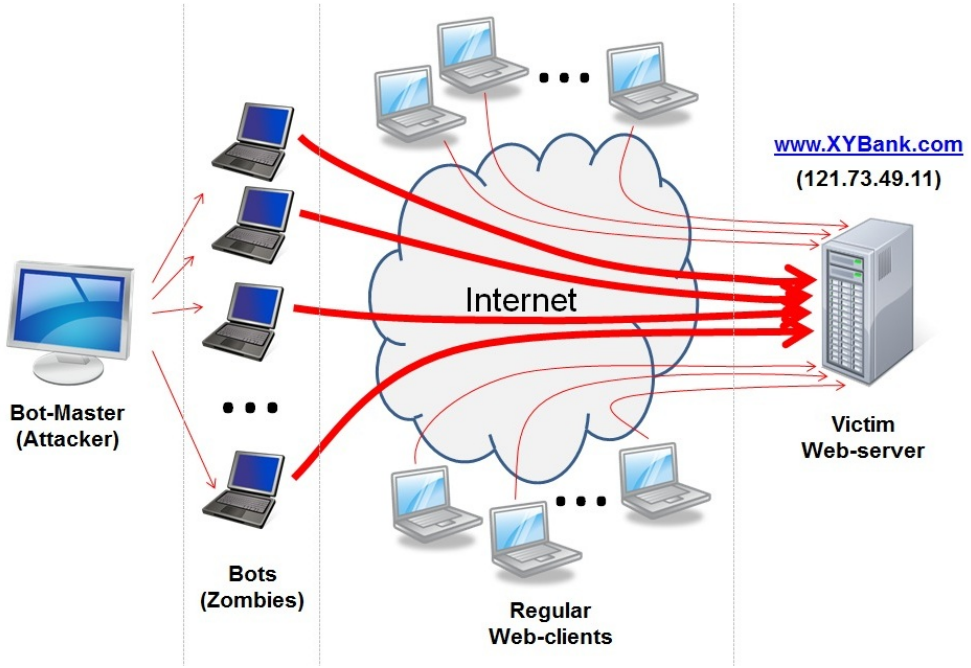
- not a practical/feasible solution for some networks …





DDoS – Defences (cont.)

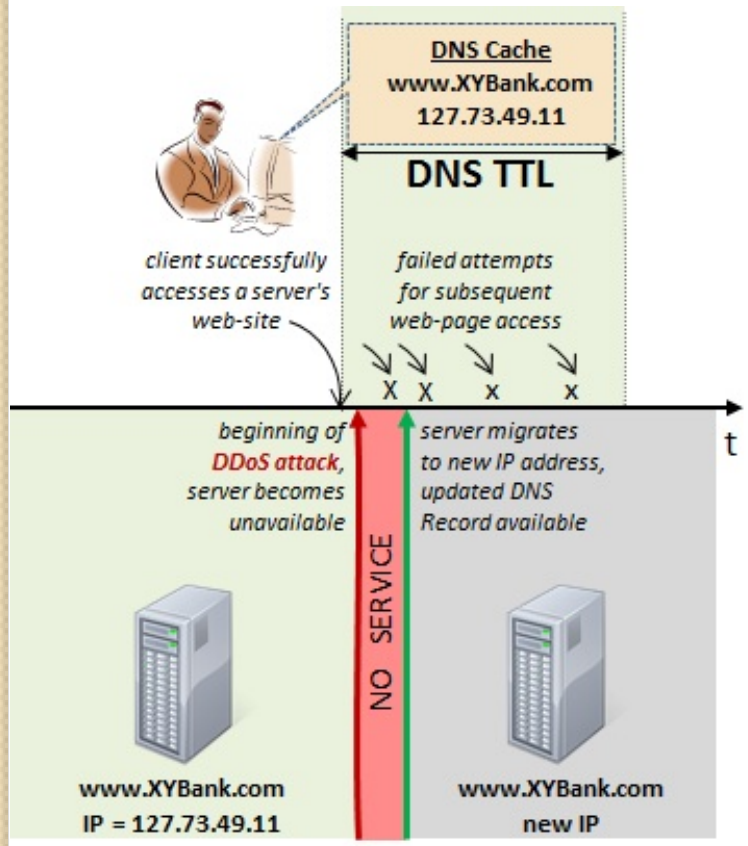
Common Problem of DDoS Defence



User/client experience is the ultimate concern of DDoS defence $\Rightarrow$ parameters controlled by server/victim site must be appropriately chosen.

DDoS and DNS TTLs

Client DNS-Cache Lock – user accessing a web-site/server before a DDoS attack, followed by server migration to a new location, are 'locked' by initially obtained DNS Record for up to TTL t.u.



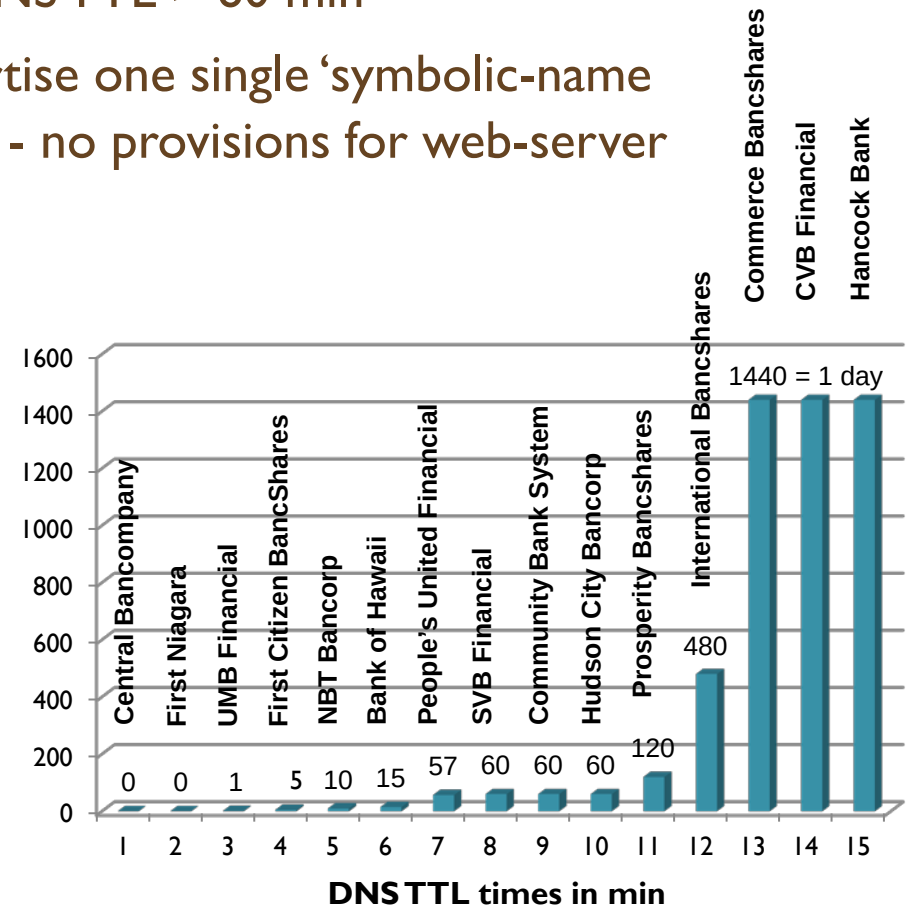
- likely actions by average user to resolve the lock:
  - → try reloading the page
  - → try closing & opening browser
  - → try opening new browser
- none of the above will affect DNS cache (help obtain new record)
- solution – in command console type: `>ipconfig /flushdns`

Empirical Study

DNS Records of 45 Major US and EU Banks

Group 1: **15 best performing US banks according to Forbes.com**

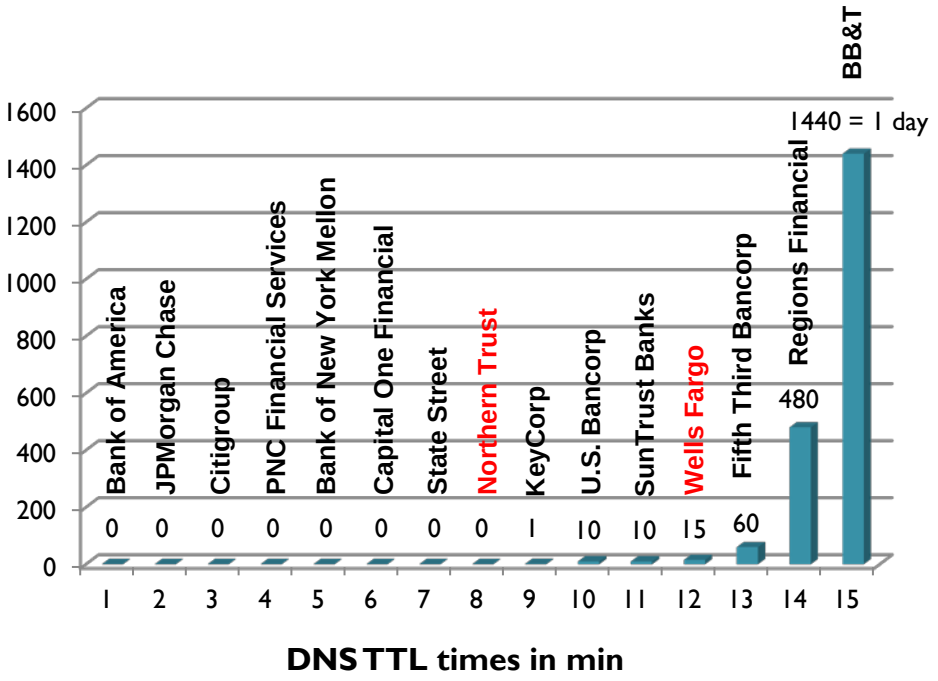
- 9 banks use DNS TTL > 60 min
- all banks advertise one single 'symbolic-name to IP' mapping - no provisions for web-server redundancy



Empirical Study (cont.)

Group 2: 15 largest US banks (asset-value) according to Forbes.com

- 3 banks use DNS TTL > 60 min
- 9 banks use DNS TTL < 1 min
- 2 banks use multiple 'symbolic-name to IP' mappings



Empirical Study (cont.)

Group 3: **15 largest EU banks according to BanksDaily.com**

- 3 banks use DNS TTL > 60 min
- 4 banks use DNS TTL = 0 min
- 2 banks use multiple 'symbolic-name to IP' mappings
- 1 bank use services of Akamai CDN