DNSSEC

Anish Patel, Jay Ganguli

What is DNS?

- Domain Name System
- DNS maps domains names to IP addresses
  - Google.com → 172.217.165.14
- Backbone of the internet

What is DNS?

Bell

ROGERS

Recursive Name Server

Client

Root Name Servers

TLD Servers

.com

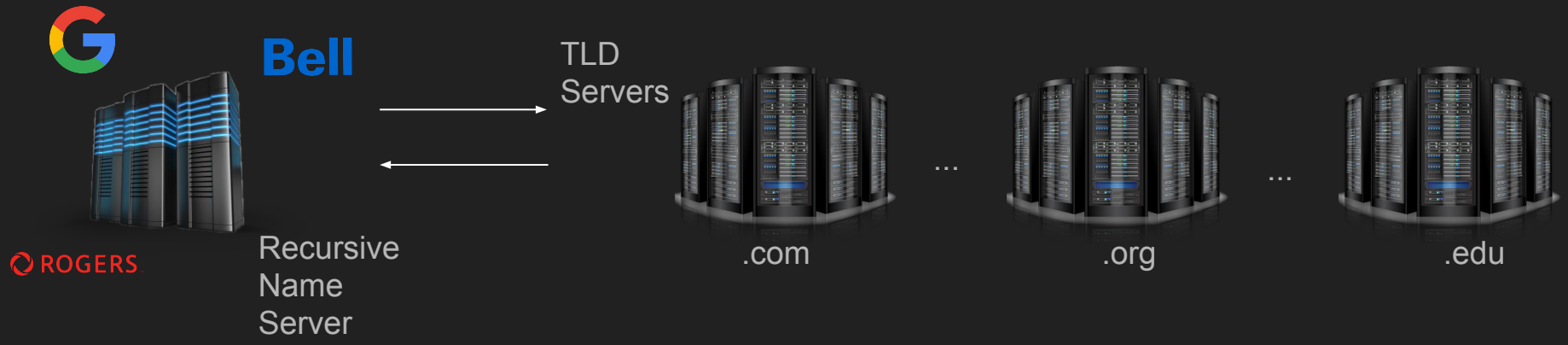
.org

.edu

Authoritative Name Servers

The Root Name Servers

- Accept a query which includes a domain name
- Redirects the recursive resolver to the appropriate TLD server
- 13 networks located around the world (these servers are always known by the recursive name servers: https://www.iana.org/domains/root/servers)
- Overseen by the Internet Corporation for Assigned Names and Numbers (ICANN) and managed by various organizations



TLD (Top-Level Domain) Servers

- Maintains information for all domain names that share a common extension
- Redirects the recursive resolver to the appropriate Authoritative Name Server
- Managed by the Internet Assigned Numbers Authority (IANA)
    - Two groups of TLD servers:
        - Generic top-level domains (.com .org .net etc.)
        - Country code top-level domains (.uk .us .ca .jp etc.)

Authoritative Name Servers

- Maintains information specific to a domain (eg: example.com)
- Provides an ip address to the requested server
    - May return an alias domain. The recursive name server will have to do a new DNS lookup in order to get an actual ip address

Alias domain: multiple domain names can point to the same server ip. When this happens, the Recursive Resolver returns the originally searched domain and whatever ip it gets. The client wouldn't know that they've been redirected.

The pros: users can access the same server from different domain names

The cons: attackers can exploit this (see in the next slides)

DNS DEMO

http://dnsviz.net

The Problem

- DNS was designed in the 80s
- Security wasn’t the primary consideration
- DNS traffic is not encrypted
- RNS has no way of authenticating responses it gets from DNS servers
- Vulnerable to DNS cache poisoning

DNS Cache Poisoning

To improve efficiency, a DNS server will cache certain domains.

But these servers have no way of guaranteeing that the ip it got is legitimate.

Attackers can leverage this. By intercepting a DNS query and providing their own malicious ip, they may cause the DNS to cache their ip to a commonly used domain name.

DNS server can “share” their cached domains with other servers, causing further damage.

DNSSEC

- Domain Name System Security Extensions
- A layer of security on top of DNS which signs responses

DNSSEC - How it works - Step 1

- Grouping DNS Records (Resource Records) into a RRSet

example.com	12.34.56.78
mail.example.com	12.34.56.78

DNSSEC - How it works - Step 1

- Grouping DNS Records (Resource Records) into a RRSet

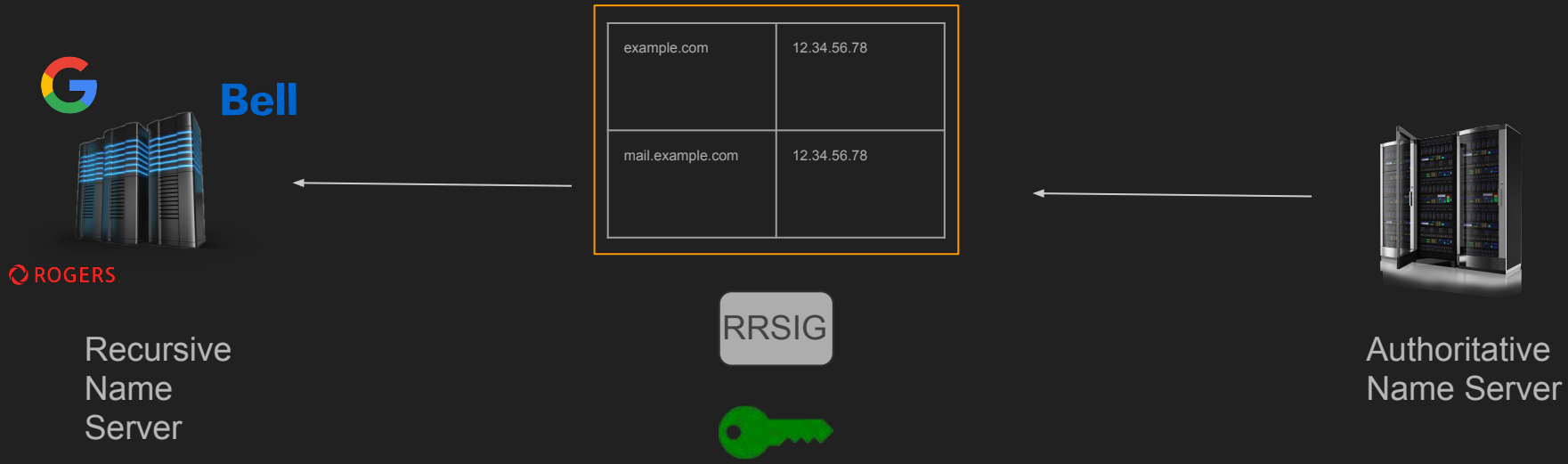
example.com	12.34.56.78
mail.**example.com**	12.34.56.78

DNSSEC - How it works - Step 2

- Zone-Signing Keys

DNSSEC - How it works - Step 2

- Zone-Signing Keys



DNSSEC - How it works - Step 3

- Key-Signing Keys

DNSSEC - How it works - Step 3

- Key-Signing Keys

RRSIG

example.com	12.34.56.78
mail.example.com	12.34.56.78

RRSIG

DNSKEY	
DNSKEY	

Recursive Name Server

Authoritative Name Server

Root Name Servers

TLD
Servers

.com ... .org ... .edu

Authoritative
Name Servers

DNSSEC - Chain of Trust

TLD

DS	Hashed KSK

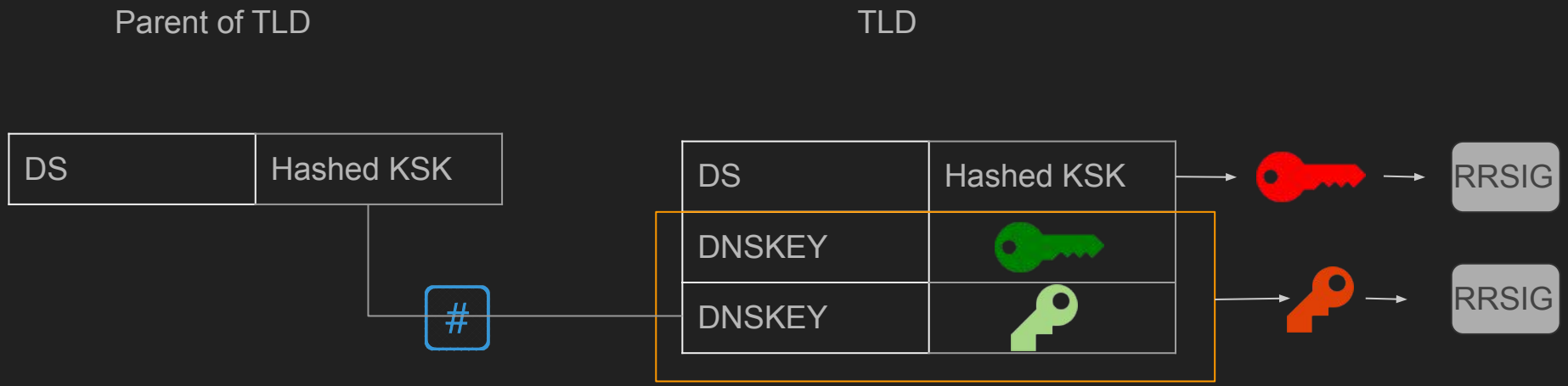
#

Authoritative
Name Servers

example.com	12.34.56.78
mail.example.com	12.34.56.78

DNSKEY	
DNSKEY	

DNSSEC - Chain of Trust



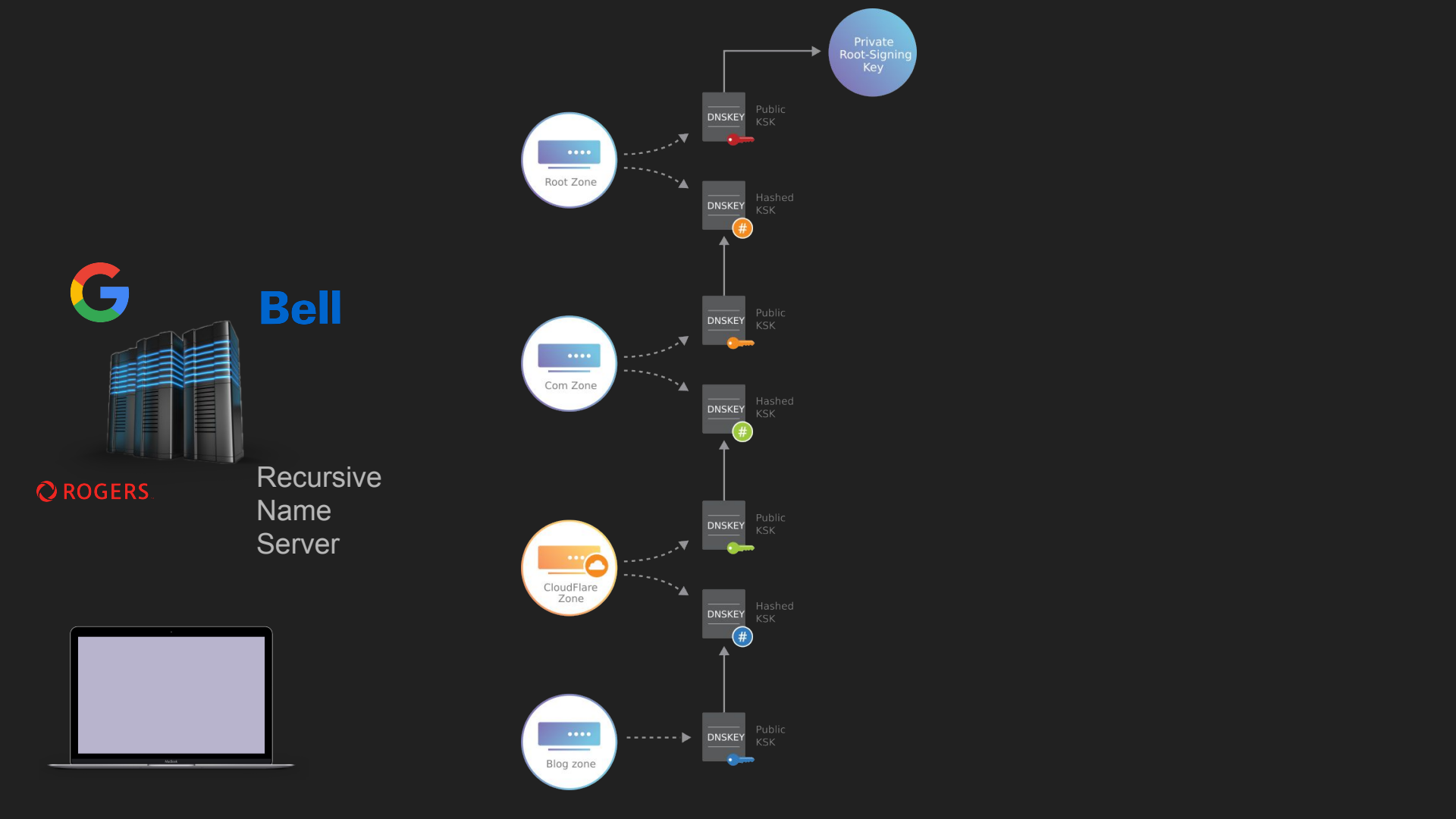
Root Name Servers

TLD
Servers

.com ... .org ... .edu

Authoritative
Name Servers


DNSSEC
IP


Private Root-Signing Key
DNSKEY
Public KSK
Root Zone
DNSKEY
Hashed KSK
DNSKEY
Public KSK
Com Zone
DNSKEY
Hashed KSK
DNSKEY
Public KSK
CloudFlare Zone
DNSKEY
Hashed KSK
DNSKEY
Public KSK
Blog zone
Bell
ROGERS
Recursive Name Server

Thank you