Operational Excellence Webinar Series

Reserve Bank Information Technology Private Limited

Securing the Bank's Internet

DNS Management Best Practices

ReBIT & **PayPal**

Panelists

Phoram Mehta
Head of Information security, Asia-Pacific region

PayPal

Vivek Srivastav
Senior Vice President, Research and Innovation

ReBIT

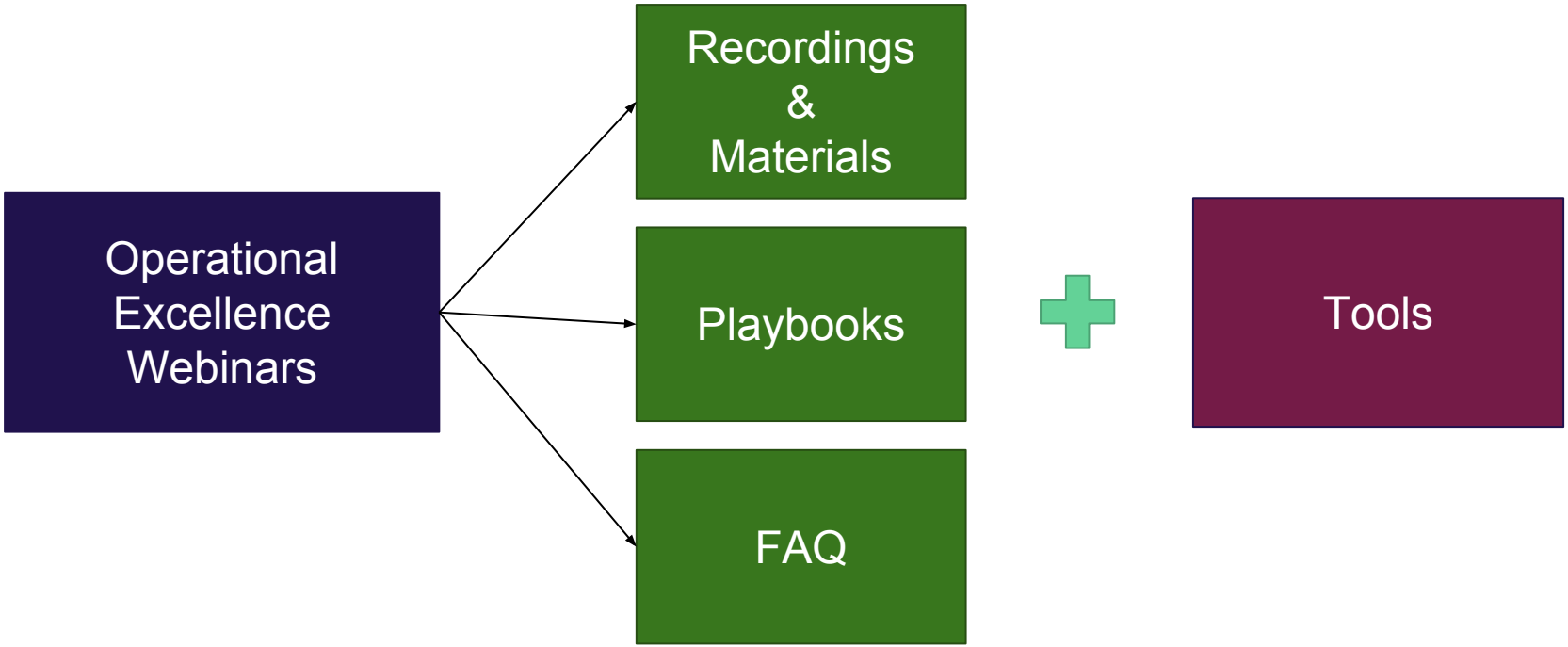
Agenda

- Brief overview/background of the Operational Excellence Program
- DNS Attacks
  - Brazilian Bank Heist - DNS Hijacking
  - DNS Cache Poisoning Attack
- DNS Overview
- PayPal: DNS Governance Case Study
- Q/A sessions

Background

ReBIT’s Operational Excellence Program

Operational Excellence Webinar



http://webinar.rebit.org.in

ReBIT's Facilitator Role

Agenda

- Brief overview/background of the Operational Excellence Program
- DNS Attacks
  - Brazilian Bank Heist - DNS Hijacking
  - DNS Cache Poisoning Attack
- DNS Overview
- PayPal: DNS Governance Case Study
- Q/A sessions

Brazilian Bank

DNS Hijack

DNS Redirect Attack on Brazilian Bank (Oct 22nd, 2016)

- DNS entries of all of the Bank's 36 online properties
  - Online Banking, Mobile Banking, ATM
- Bank was unable to send emails to its customers
- The look-alike website had valid certificates from Let's Encrypt
- Malware dropped on customer's PC
- Likely cause
  - DNS Hijacking: social engineering, brute force
  - Cache Poisoning

Security Considerations

- Do you **manage your own** DNS?
- Does your registrar provides **MFA**?
- Does your registrar provides "**registry lock**"?
- Do you use **strong password** for DNS admin account at your registrar?

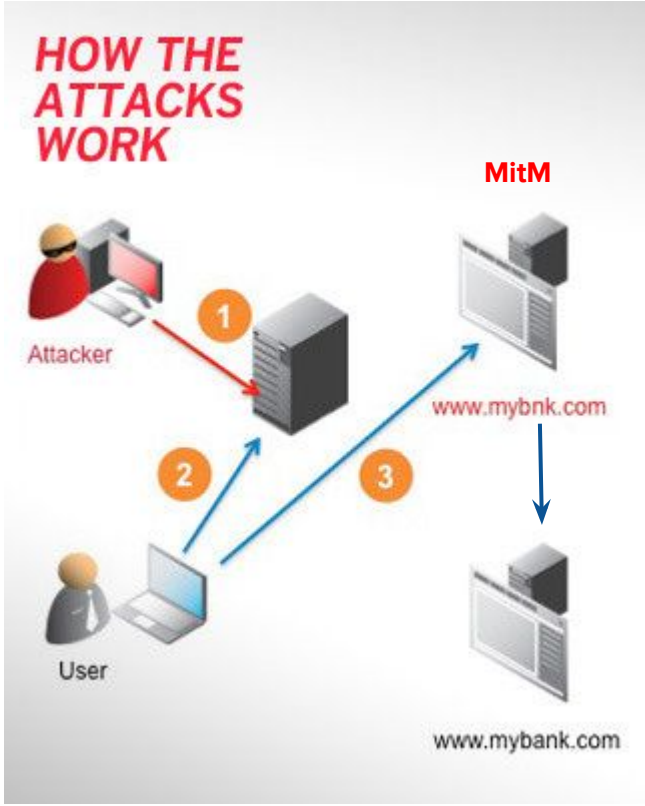
DNS Hijacking

Modifies DNS record settings (most often at the domain registrar) to point to a rogue DNS server or domain.

- Attacker gains access to the DNS record settings and modifies the record to point the IP address to a malicious website
- User tries to access a legitimate website www.mybank.com
- User gets redirected to bogus site controlled by hackers that looks a lot like the real thing.

Impact

- Hackers acquire user names, passwords and credit card information



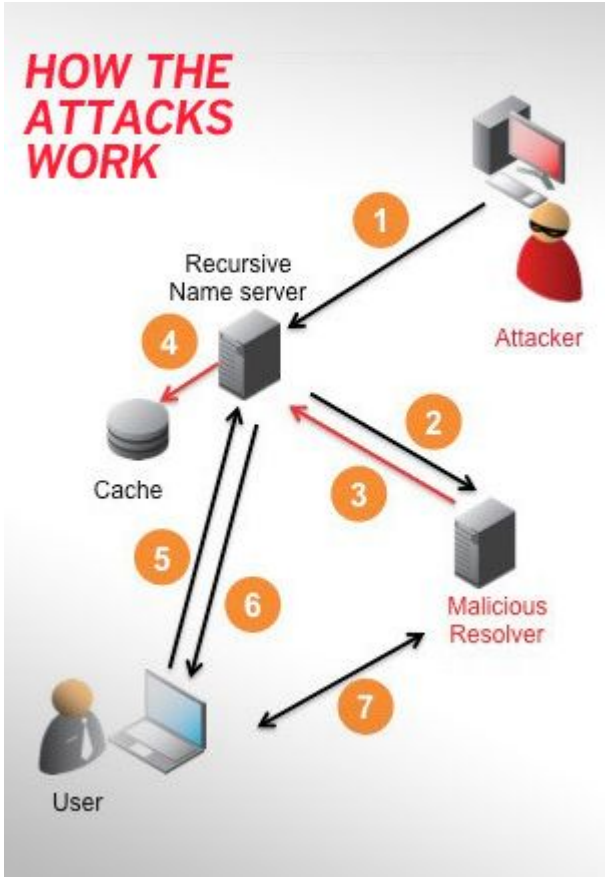
Cache Poisoning Attack

Corruption of the DNS cache data

1. Attacker queries a recursive name server for IP address of a malicious site
2. The recursive server does not have the IP address and queries a malicious DNS resolver
3. The malicious resolver provides requested rogue IP address and also maps the rogue IP address to additional legitimate sites (e.g. www.mybank.com)
4. The recursive name server caches rogue IP address as the address for www.mybank.com
5. User queries the recursive server for IP address of www.mybank.com
6. The recursive server replies to user with cached rogue IP address
7. Client connects to site controlled by attacker, thinking it is www.mybank.com

Impact:

Logins, passwords, credit card numbers of the user can be captured



Agenda

- Brief overview/background of the Operational Excellence Program
- DNS Attacks
  - Brazilian Bank Heist - DNS Hijacking
  - DNS Cache Poisoning Attack
- DNS Overview
- PayPal: DNS Governance Case Study
- Q/A sessions

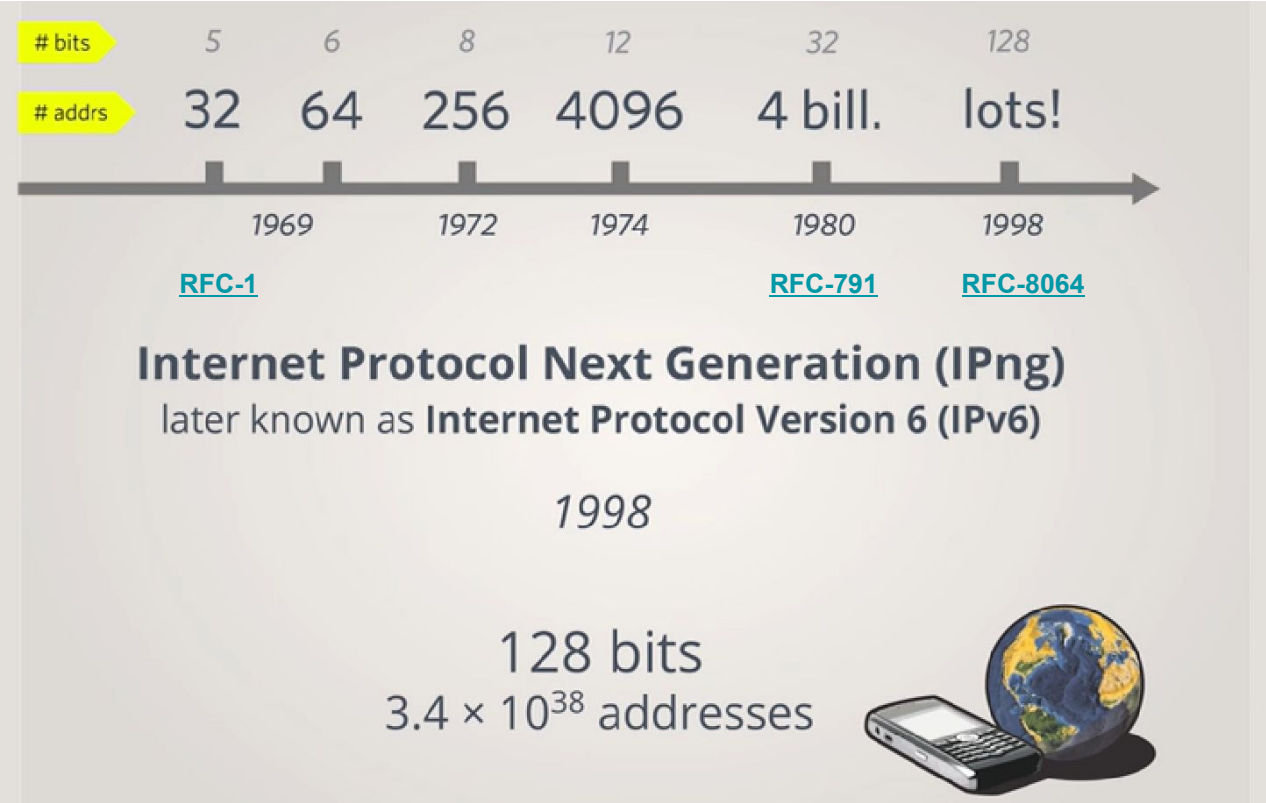
DNS Overview

Hierarchy & Zones

DNS Overview

- **Domain Name Servers** are distributed hierarchical system to convert domain names to IP Addresses
- **DNS Components**
  - DNS Resolver
  - Name Servers
  - Resource Records

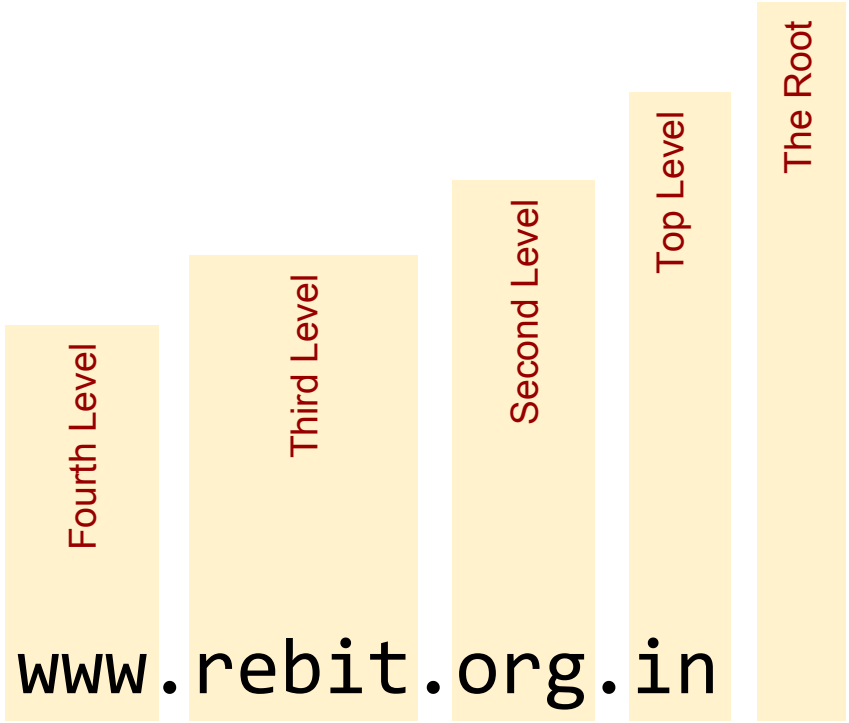
IP Addresses



Source: ICANN

Domain Name

115.248.45.13



Name Resolution Mechanism

1	Where is www.rebit.org.in
2	Don’t know, ask .in server

Root server

3	Where is www.rebit.org.in
4	Don’t know, ask .org.in server

.in server

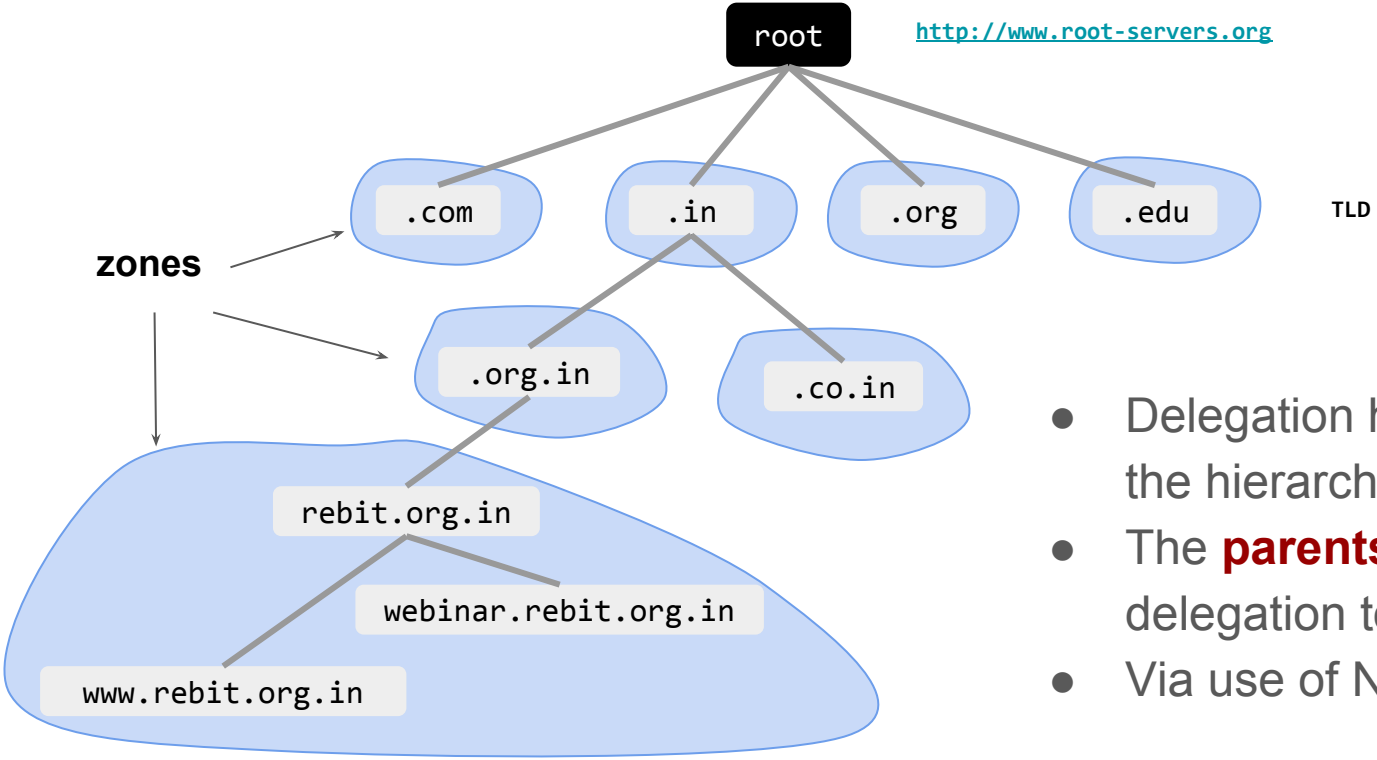
5	Where is www.rebit.org.in
6	Ask .rebit.org.in server

.org.in server

7	Where is www.rebit.org.in
8	It’s at 115.248.45.13

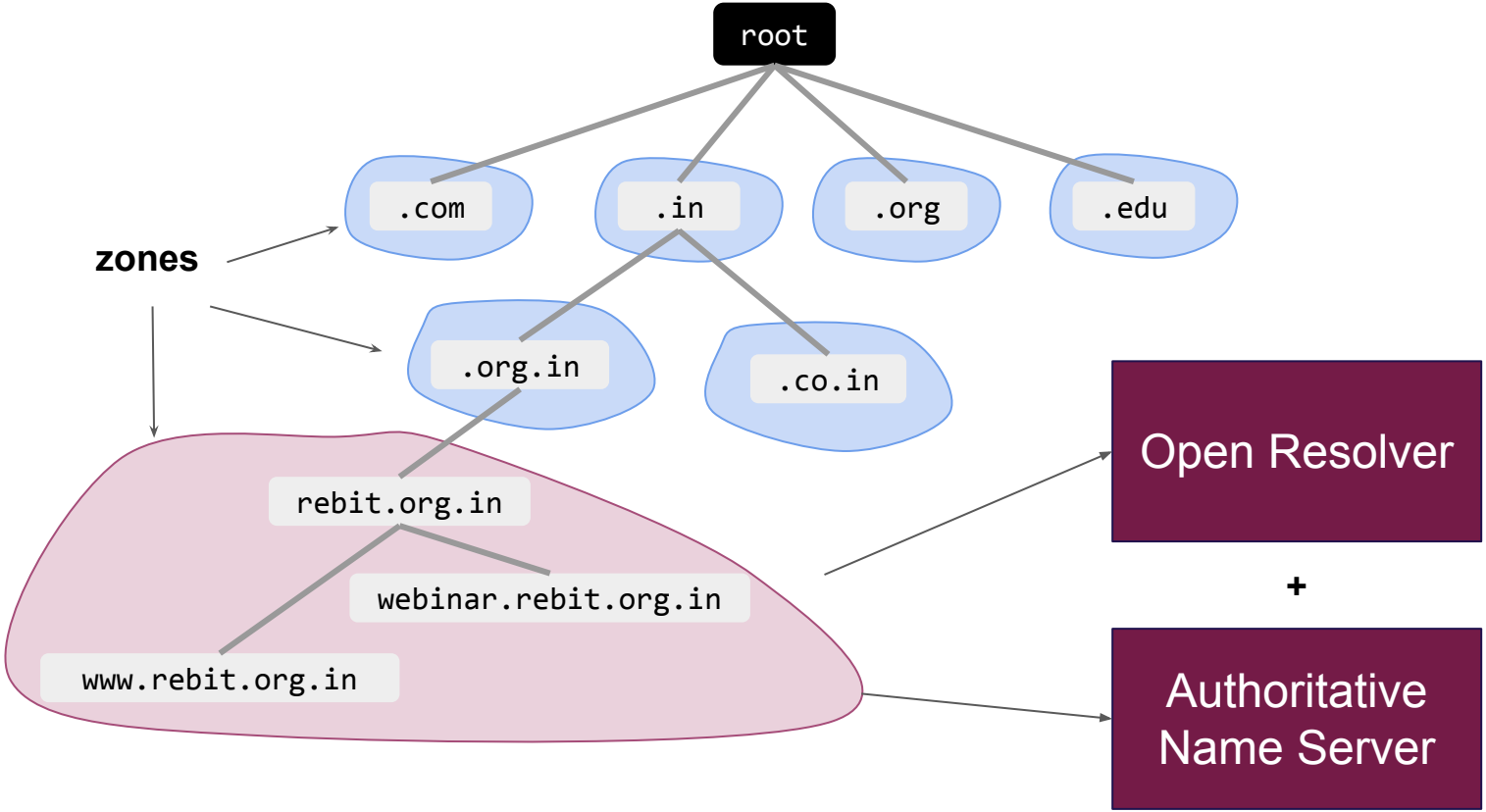
.rebit.org.in server

DNS Hierarchy



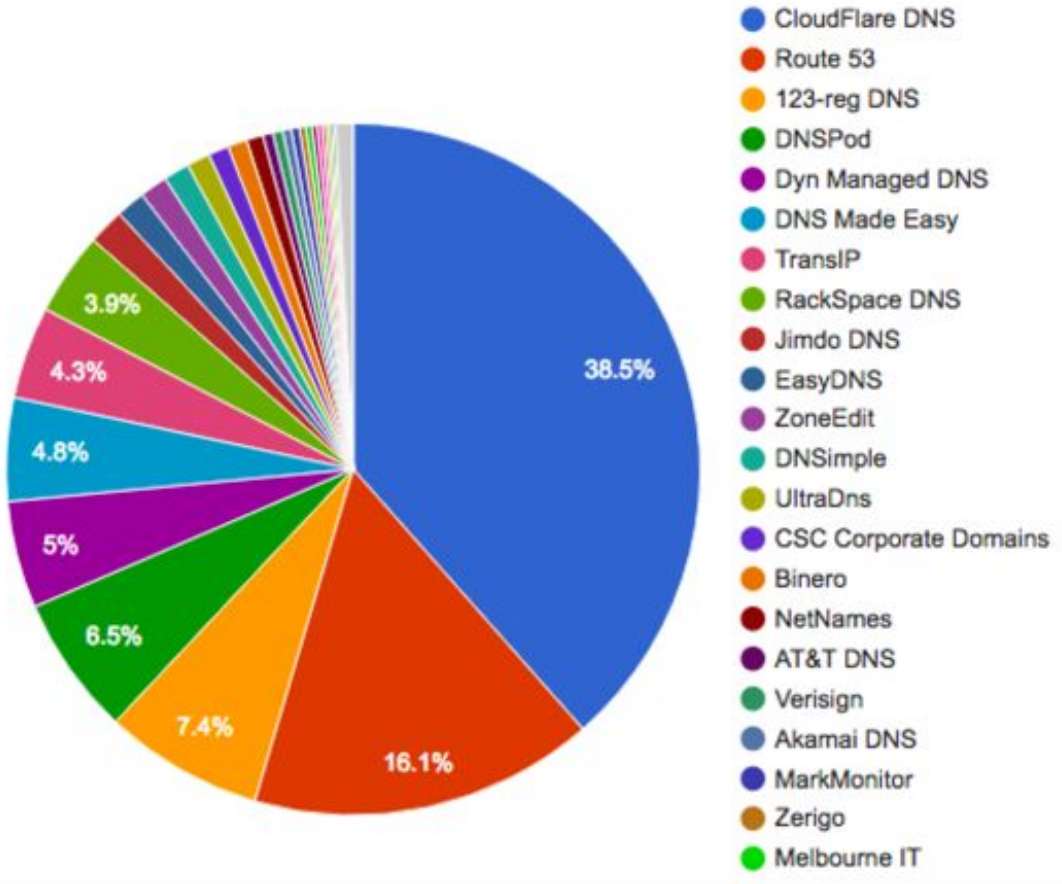
- Delegation happens down the hierarchy
- The **parents** makes the delegation to **child zones**
- Via use of NS records

DNS Resolvers



Open Resolvers

An open DNS server is a DNS server which is willing to resolve recursive DNS lookups for anyone on the Internet.



The Open Resolver Project

Open Resolver Project

Open Resolvers pose a significant threat to the global network infrastructure by answering recursive queries for hosts outside of its domain. They are utilized in DNS Amplification attacks and pose a similar threat as those from Smurf attacks commonly seen in the late 1990s.

We have collected a list of 32 million resolvers that respond to queries in some fashion. 28 million of these pose a significant threat (as of 27-OCT-2013). Detailed History and Breakdown

Agenda

- Brief overview/background of the Operational Excellence Program
- DNS Attacks
  - Brazilian Bank Heist - DNS Hijacking
  - DNS Cache Poisoning Attack
- DNS Overview
- PayPal: DNS Governance Case Study
- Q/A sessions

DNSSEC

Brief Overview

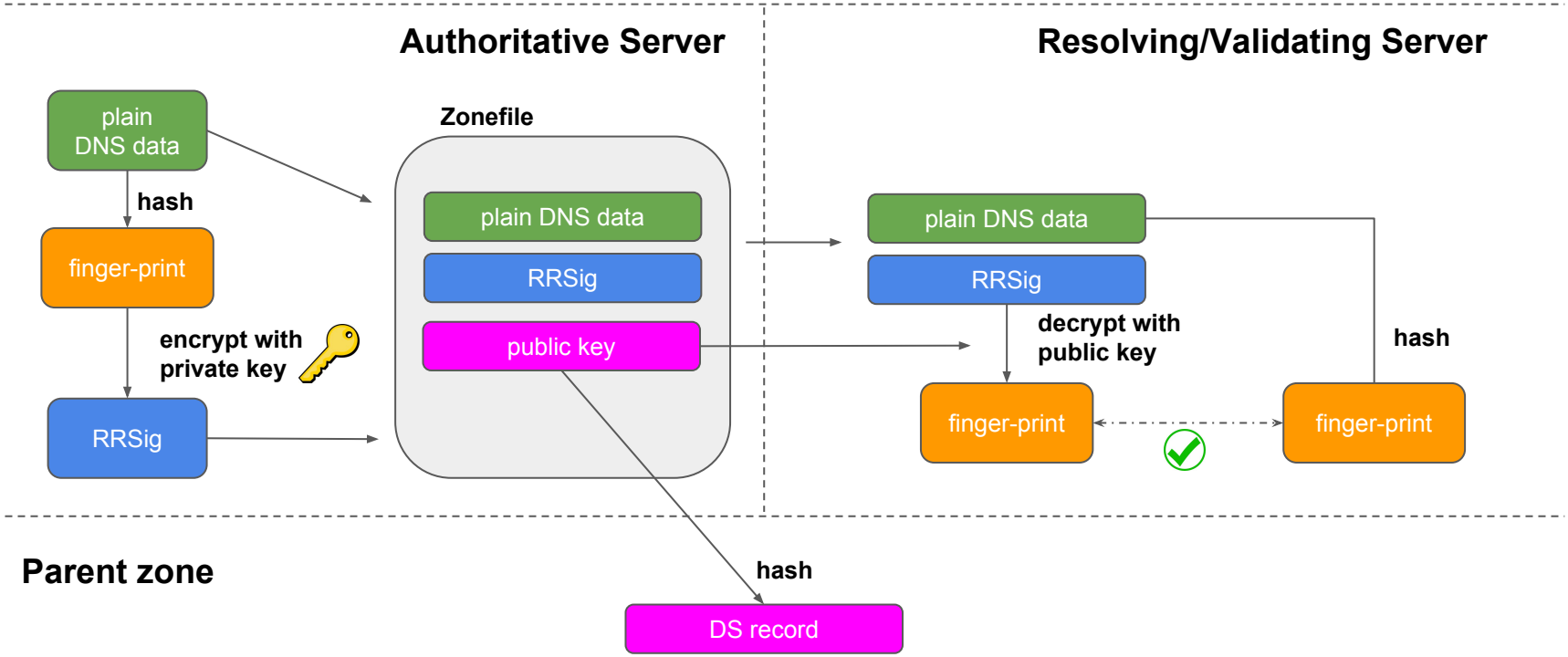
Email servers use DNS to route their messages. In September 2014, researchers at CMU found email supposed to be sent through Yahoo!, Hotmail, and Gmail servers routing instead through rogue mail servers.

Attackers were exploiting a decades-old vulnerability in the Domain Name System (DNS)—it doesn’t check for credentials before accepting an answer.

What is DNSSEC

- A security extension to authenticate DNS data
- DNS data is cryptographically signed by the owner of the DNS zone
- The recipient of the data can validate the signature to ensure
  - The data has not been changed since signing
  - That the data comes from the owner of the private key for the domain
- The recipient of DNS data can be a DNS resolver, an operating system stub-resolver or an application

DNSSEC in a nutshell



DNS Governance Best Practices (RFC 1912)

- Enter the correct e-mail address of the responsible person for each zone you add to or manage on a DNS server (SOA record)
- Make sure that you have at least two servers hosting each zone
- Make sure your PTR and A records match

DNS best practices

- Decide who can resolve Internet host names
- Don’t co-locate internal and external zones
- Lock down the DNS cache
- Enable recursion only where it is needed
- Restrict DNS server to listen on specific addresses
- Consider using a private root hints file
- Randomize your DNS source ports
- Be aware of the Global Query Block list
- Limit zone transfers
- Take advantage of Active Directory integrated zone security

Backup Slides

References

- Secure Domain Name System (DNS) Deployment Guide
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf
- 13 root name servers operated by 12 independent organisations
  http://www.root-servers.org/
- https://tools.ietf.org/html/bcp38
- http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

Resources

- DNS
  - RFC 1034, RFC 1035, RFC 2081, RFC 4033-4035
- Authoritative Server Operations
  - RFC 2010, RFC 2870
- Operation of Anycast service
  - RFC 4786