September 24, 2014

DNSSEC: How far have we come?

Nick Sullivan (@grittygrease)

Motivation

- DNS is insecure

- DNSSEC has been proposed to fix it
- How does DNSSEC work?
- What are the pros/cons?
- How is deployment going?

Background on DNS

The Internet’s phone book

The Domain Name System

- Distributed key value database

- Authority delegation via hierarchy
- Ask a question, get an answer or the right place to ask the question

The Domain Name System

- Question:

"What's the IP address of example.com?"

- Answers:

"93.184.216.119" (A record)

or

Here's who you talk to: a.iana-servers.net (NS record)

or

This domain does not exist

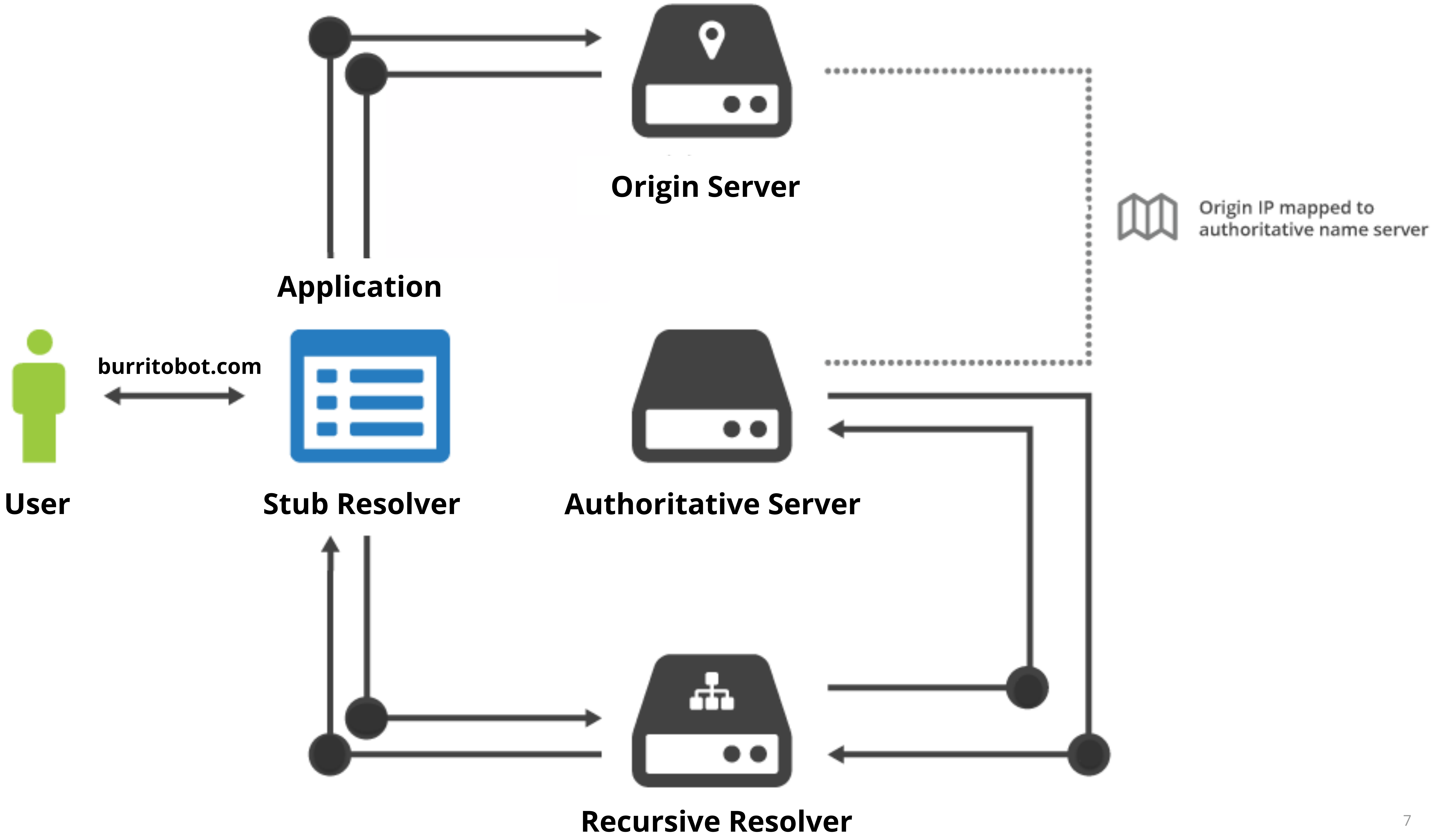
In hex

- The raw DNS request is a UDP packet that looks more like:

```
0x0000: 27e1 0100 0001 0000 0000 0000 0765 7861 ‘............exa
0x0010: 6d70 6c65 0363 6f6d 0000 0100 01        mple.com.....
```

- The response looks like this:

```
0x0000: 27e1 8180 0001 0001 0000 0000 0765 7861 ‘............exa
0x0010: 6d70 6c65 0363 6f6d 0000 0100 01c0 0c00 mple.com........
0x0020: 0100 0100 0031 f500 045d b8d8 77        .....1...]..w
```



Origin Server
Origin IP mapped to
authoritative name server
Application
burritobot.com
User
Stub Resolver
Authoritative Server
Recursive Resolver

Stub Resolvers

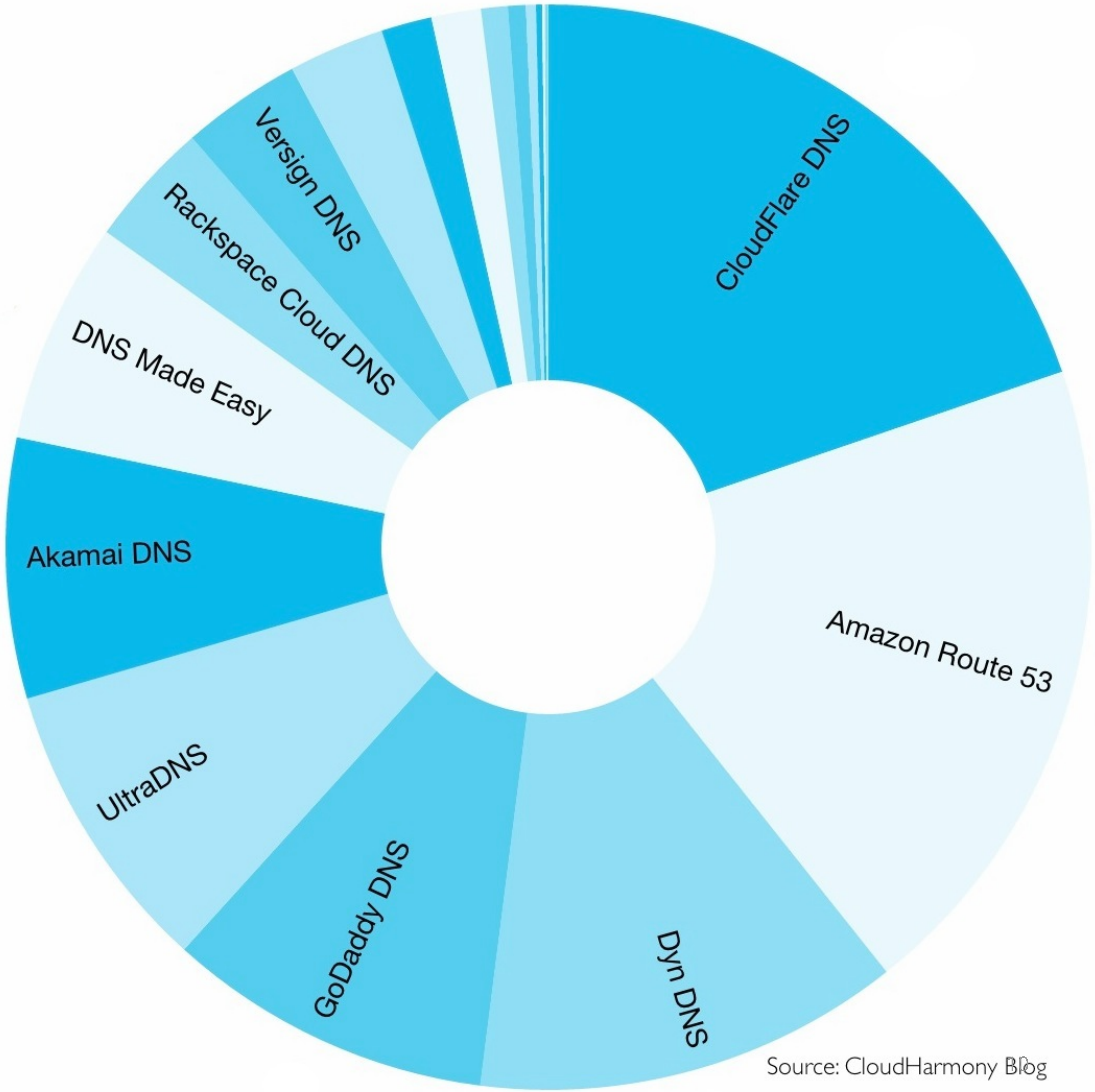
- The application interface with DNS
- Simple cache
- Being replaced by recursive resolvers on end-user hosts
  - mDNSReponder on OS X
  - Microsoft DNS Client on Windows
  - Unbound on Linux

Recursive Resolvers

- Google Public DNS
  - 8.8.8.8
  - 8.8.4.4
- OpenDNS
  - 208.67.222.222
  - 208.67.220.220
- Your local ISP

Authoritative Servers

Alexa Top 10,000 DNS Marketshare - 1 Sep 2014



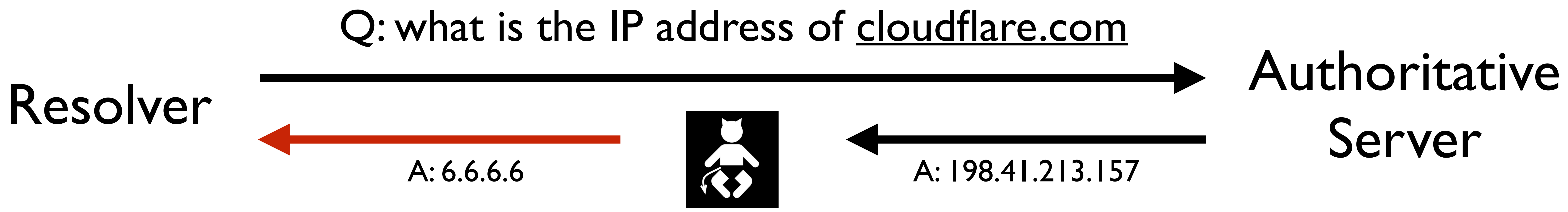
Source: CloudHarmony Blog

Why is DNS insecure?

Kaminsky's attack and more

Man-in-the-middle

- Answers can be modified
- Requires privileged network position



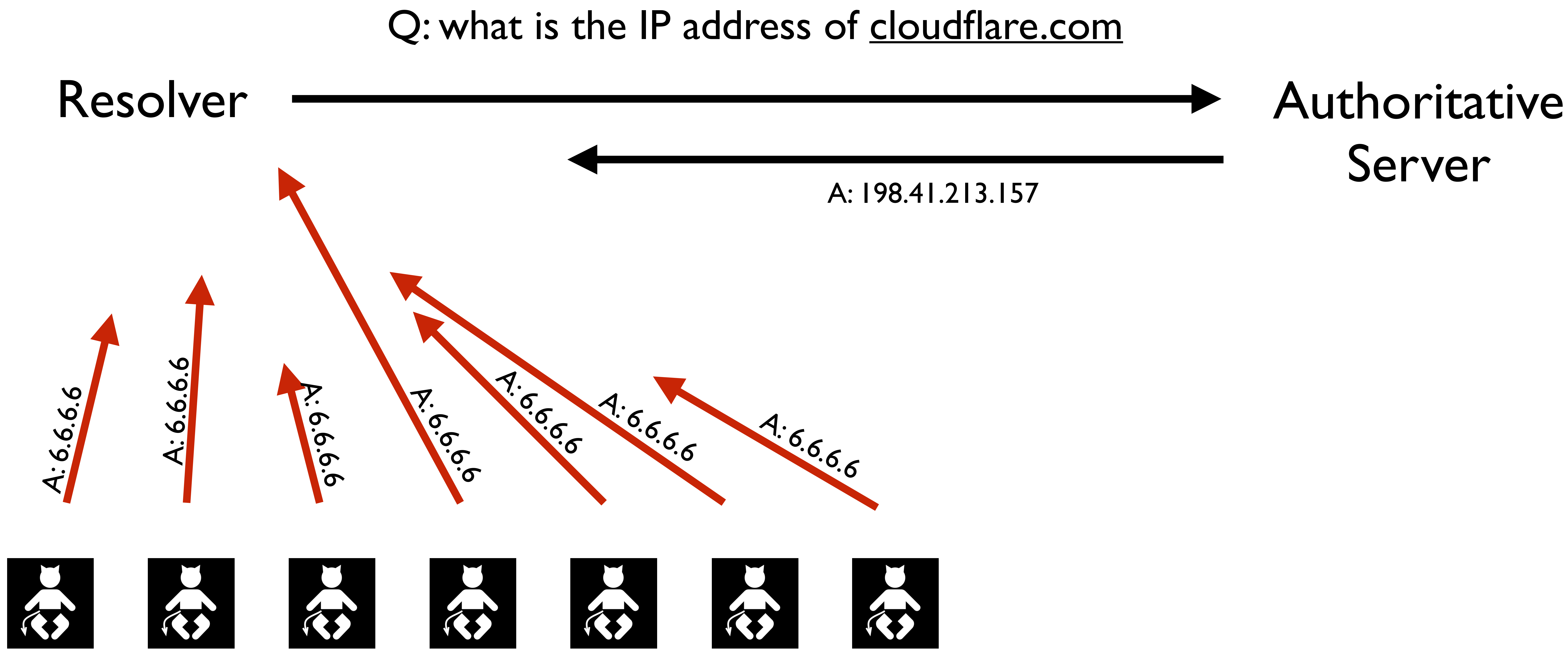
Cache Poisoning (Kaminsky's attack)

- DNS queries use spoof-able UDP

- Resolver asks authoritative server for answer
- Attacker answers first with spoofed IP of authoritative server

Cache Poisoning (Kaminsky's attack)

- DNS queries use spoof-able UDP



Real Life Attacks

- Attack this month
- Detected via passive DNS


virus BULLETIN Covering the global threat landscape

Blog | Bulletin | VB100 | VBSpam | VBWet

DNS cache poisoning used to steal emails

Call to use end-to-end encryption and to deploy DNSSEC.

DNS is sometimes called 'the phone book of the Internet'. If true, the
relatively ea

Whether it i
cache poiso
and potentia

But DNS do
email. Being

CERT | Software Engineering Institute | Carnegie Mellon University

Work Areas | Engage with Us | Training | About Us | News | Careers

Home › CERT Blogs › CERT/CC › Post

CERT/CC **BLOG**

Probable Cache Poisoning of Mail Handling Domains

By Jonathan Spring on 09/10/2014 | Permalink

Hi, this is Jonathan Spring with my colleague Leigh Metcalf. For some time now, we've been working through a pr
found, but it's time to discuss it more broadly. Using our passive DNS data source, we can observe cache poison
we really observe are changes in the answers that are returned for certain domains, but after consulting with vario
experts, we believe the only behavior these changes indicate is a successful cache poisoning attack.

The mechanism used to poison the answers is not clear. We see only responses, not queries, and figuring out the
mechanism requires visibility into the queries. This limited visibility is one reason to disclose what we've found so t
can look for the root cause.

Real Life Attacks

- Very convincing phishing sites
- Redirecting email

DNSSEC

Security for DNS

DNSSEC

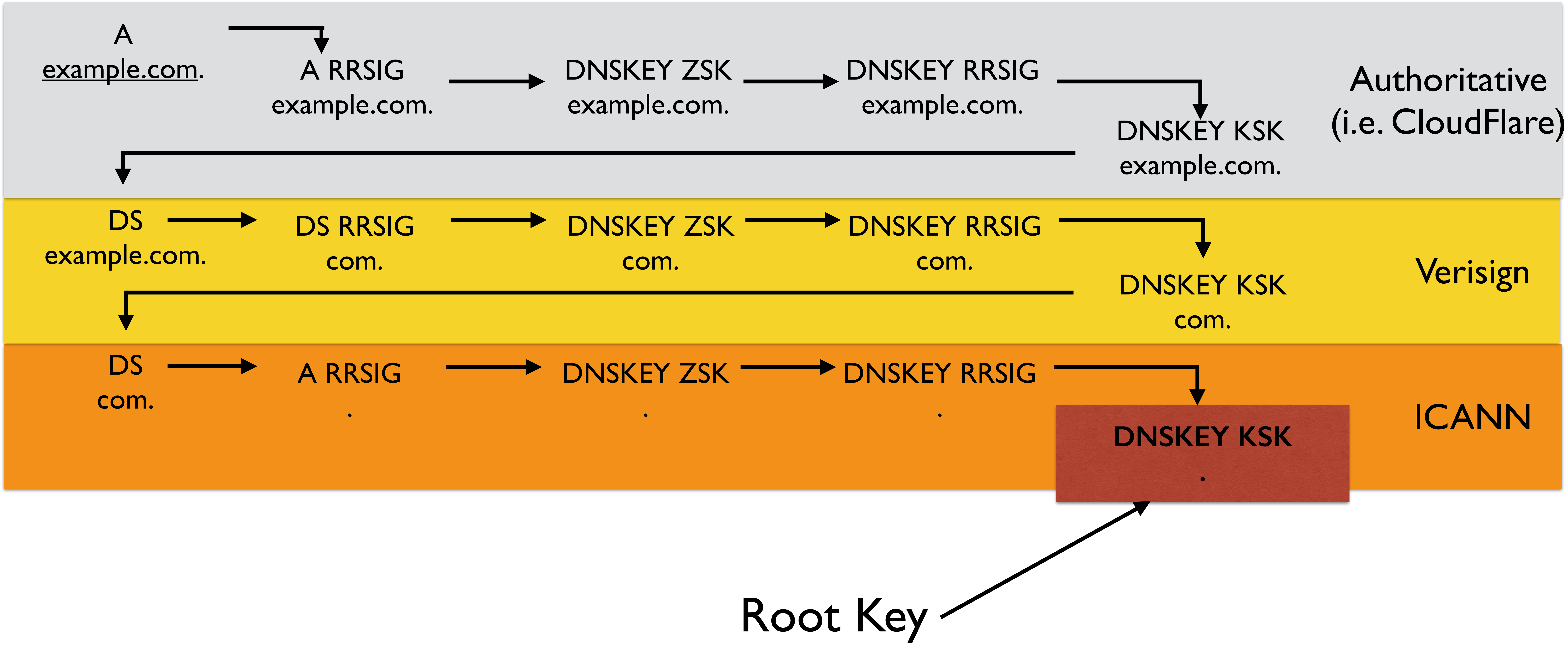
- DNS + Digital Signatures
- Chain of trust through on natural DNS hierarchy
- Authentic, not private

- Original RFC in 1997
- DNSSECbis in 2005

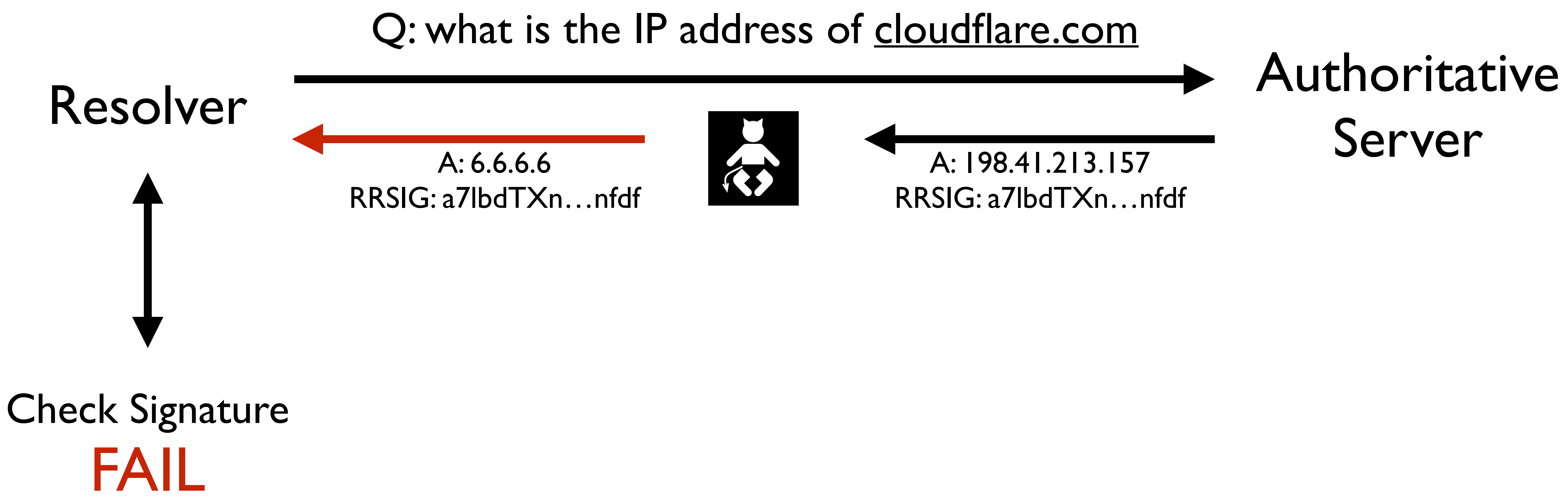
New records

- RRSIG: digital signature of a set of answers
- DNSKEY: public key, comes in two flavors
  - key signing key (KSK)
  - zone sigining key (ZSK)
- DS: delegated signer, hash of DNSKEY
- NSEC(3): proof of non-existence

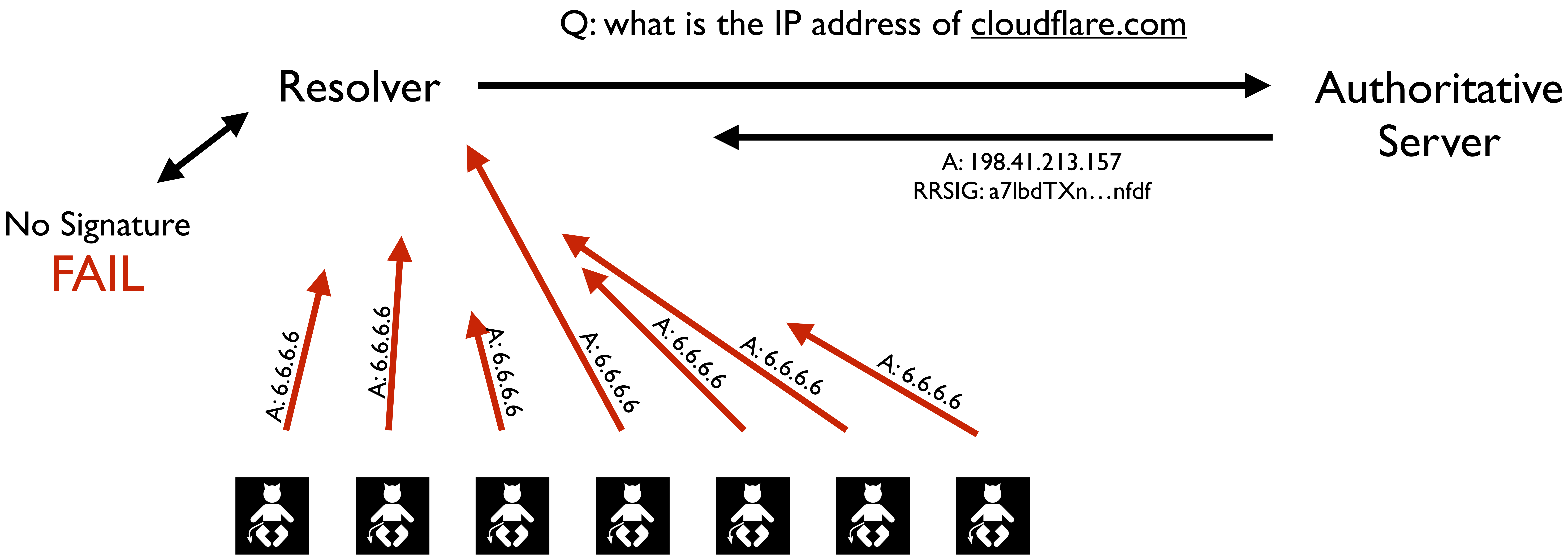
DNSSEC signature verification



Man-in-the-middle thwarted



Cache Poisoning thwarted



Problem solved, right?

- Not so fast…

Problems

DNSSEC controversies

Main Problems

- Zone privacy
- Reflection/Amplification
- Last hop
- Complexity/Risk

Zone privacy

- NSEC walking
- NSEC3 dictionary attack
- Live signing to the rescue

Zone Walking

- NSEC: records to prove the nonexistence of records
- Signs pair of records, claim no records exist between
- “Covers” the whole zone

Zone Walking

```
Q: A tx.ietf.org

A: trustee.ietf.org.  1683  IN NSEC  www.ietf.org. A MX AAAA RRSIG NSEC

Q: A wwwa.ietf.org

A: www6.ietf.org.     938   IN NSEC  xml2rfc.ietf.org. CNAME RRSIG NSEC
```

- Walk the whole zone

Zone Dictionary Attack

- In NSEC3, it’s the hash of the zone.
- Walk the whole zone to collect all the hashes
- Hash and compare dictionary offline

Solution: Live signing + “white lies”

- Create NSEC(3) and RRSIG records on the fly
- Sign smallest possible gap, i.e.:

```
somethinfzzzzzzzzzzzzzzzzzz.com to
something000000000000000001.com
```

Live signing problems

- Key management
  - Is deploying keys safe?
  - Hardware Security Modules (HSMs)?
- CPU usage
  - Mitigated with modern hardware and ECDSA keys
- Implementations
  - Not available in BIND

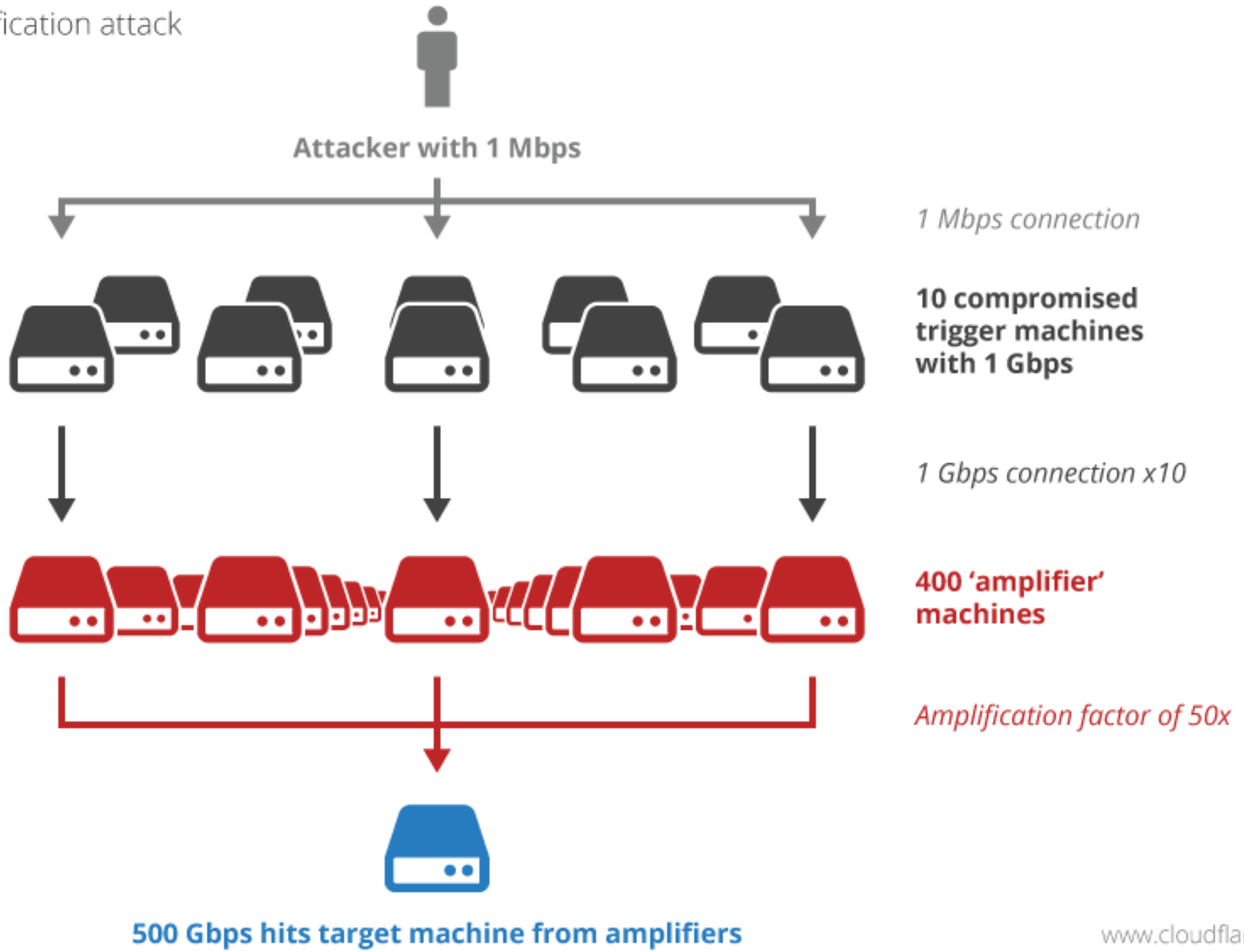
Amplification/Reflection

- DNS amplification attacks

UDP is unauthenticated

- Small requests can result in big responses in DNSSEC
- Especially ANY and DNSKEY questions
- UDP is unauthenticated (some networks do not implement BCP 38)

Amplification attack



Solution: Use TCP?

- RFC 5966, 2010-08, DNS Transport over TCP:

"[...] TCP is henceforth a REQUIRED part of a full DNS protocol implementation."

- Not enough servers support it (16% don't retry [2012, circleid])
- Worries of slowdown for TCP handshake
  - T-DNS claims this is unfounded (http://www.isi.edu/ant/tdns/index.html)

Solution: Use Elliptic Curves?

- Elliptic curve keys are smaller than RSA keys
- Smaller amplification ratio

- Universal support lagging

Last hop

- Stub resolver to recursive resolver message is unauthenticated
- Problem going away: validating resolvers on end user machines

- In the meantime:
  - DNSCurve
  - TLS

Complexity/Risk

- Changes at the network protocol layer are scary
- Schedule for rotating keys
- Mistakes here can cost a lot of money

Problems

- ~~Zone privacy~~
- Reflection/Amplification
- ~~Last hop~~
- Complexity/Risk

vs

- Security and Trust
- More?

DNSSEC extensions

Replacing the Certificate Authority PKI with the DNS PKI

DNS-based Authentication of Named Entities (DANE)

- Put the website certificate in DNS
- Can replace the certificate authority system
  - TURKTRUST (2011), DigiNotar (2011), Indian Gov (2014)

- Questions:
  - Trust chain for sites runs through the TLDs (e.g. Libya .ly, Indian Ocean .io, ...)

DNSSEC deployment

Where are we today

Requirements to work

- Trust chain established
- Domains need to be trusted
- Resolvers need to check
- Users have to be alerted

Signing the root

- Complicated “key ceremony” process managed by ICANN
- The first root zone keys published on July 15, 2010
- Root key:

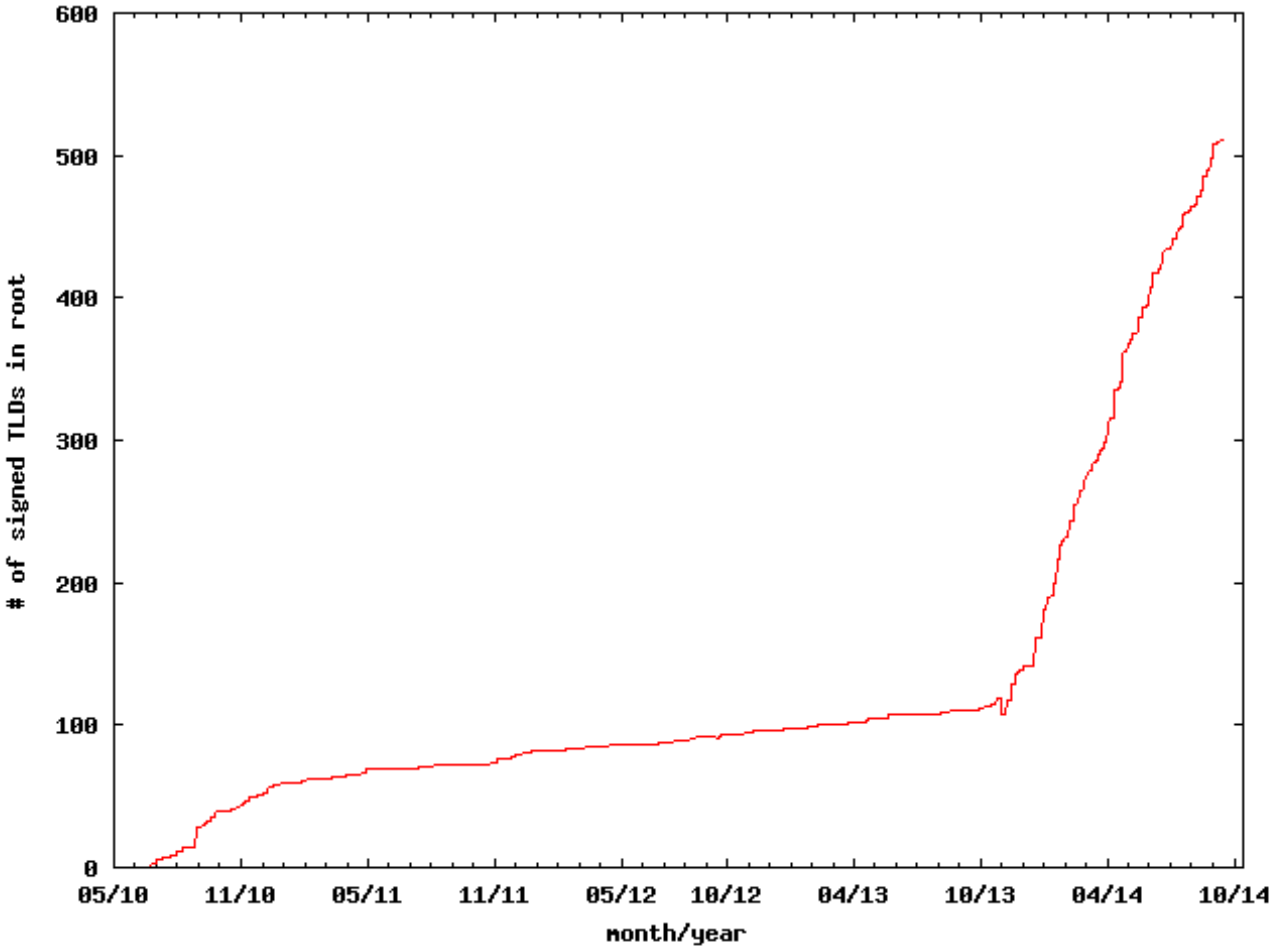

```
AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
QxA+Uk1ihz0=
```

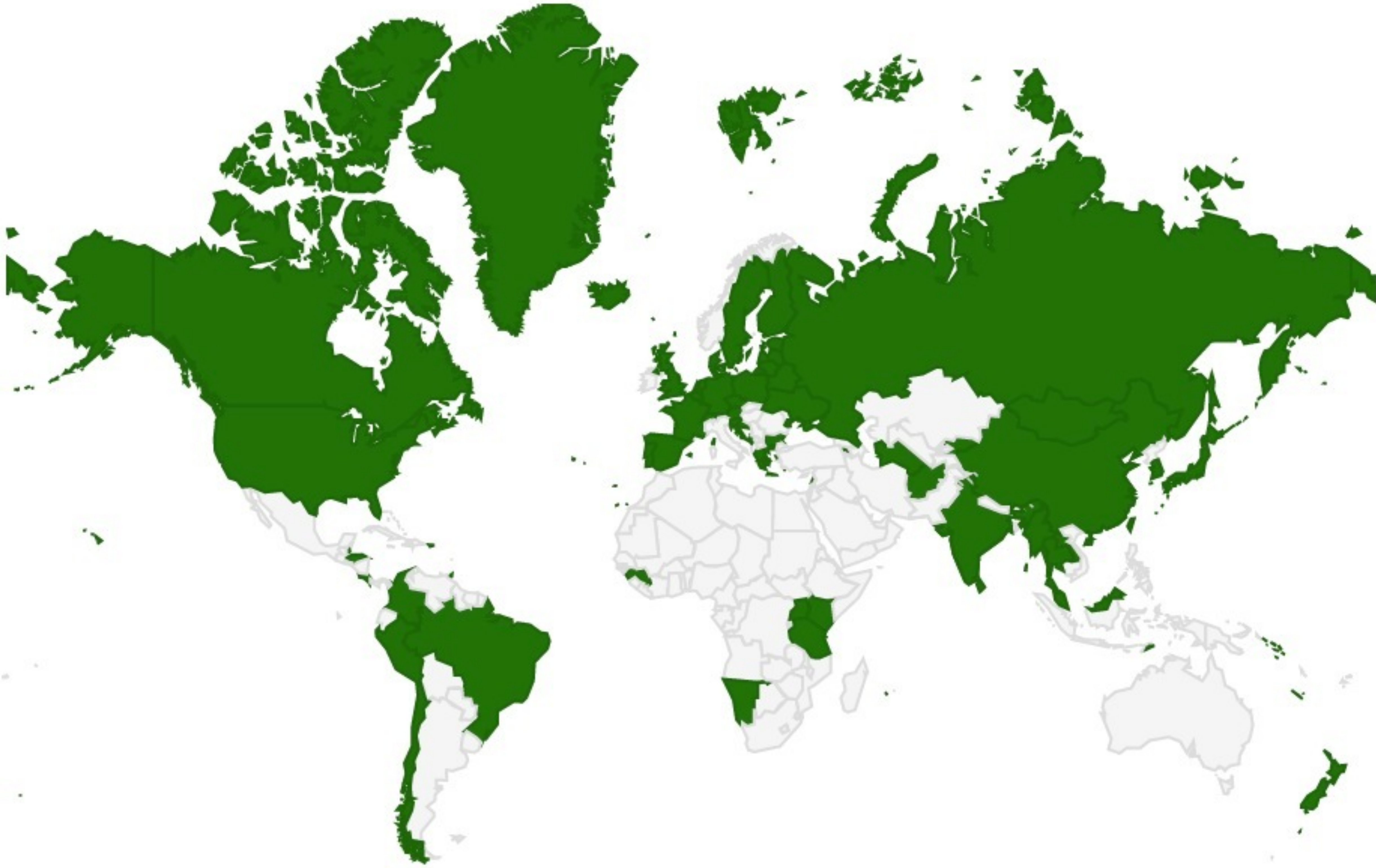

CLOUDFLARE

TLDs

- June 2009: .org was signed
- Others followed suit
- All new TLDs are required to be signed at launch

TLDs signed (http://rick.eng.br/dnssecstat/)



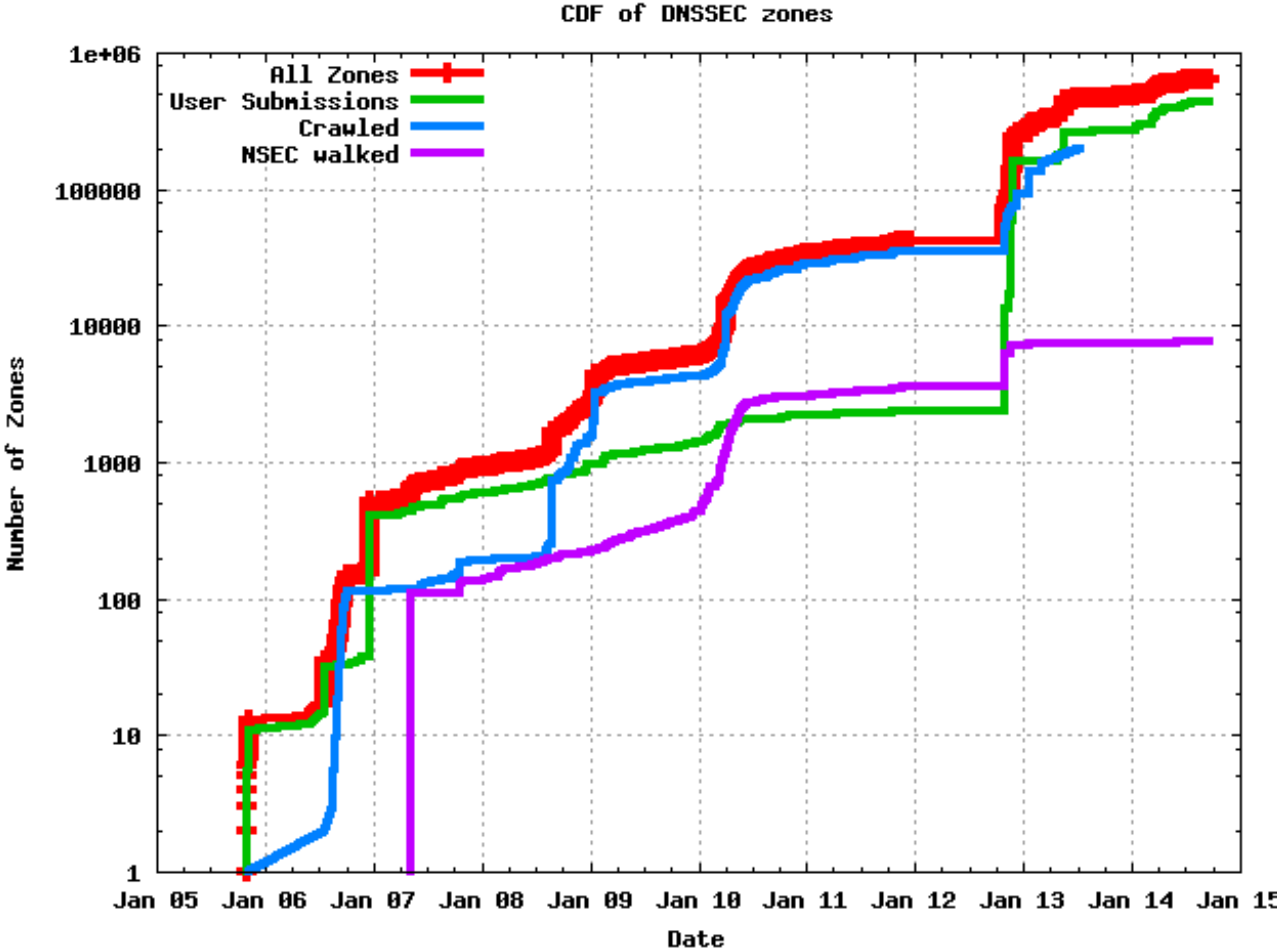


Individual Domains

- Growing numbers
- 0.3% of .com domains (~400,000)
- 0.5% of .net domains (~70,000)
- 6.9% of .eu names (~260,000)
- 1 million+ .nl names

Individual Domains (http://secspider.cs.ucla.edu/growth.html)

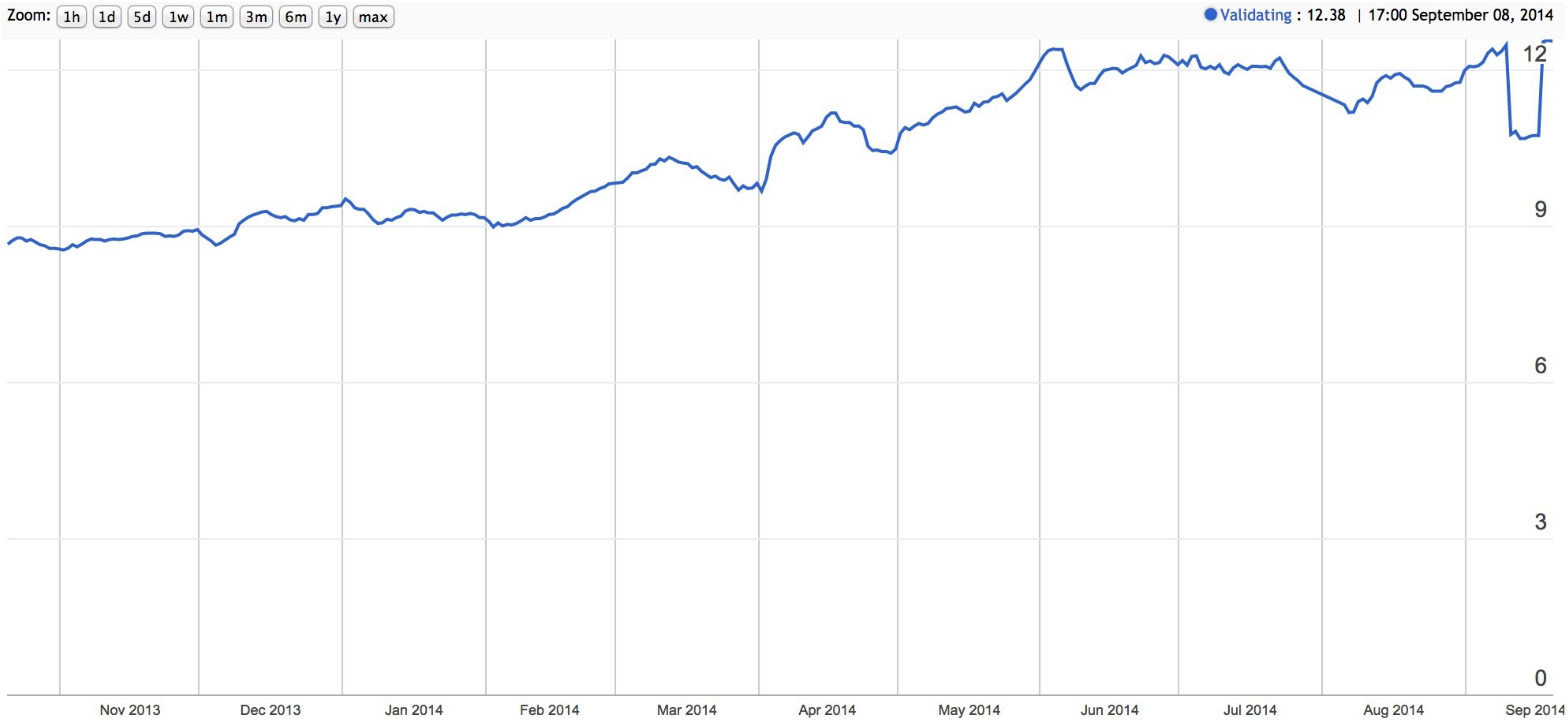
- Under a million
- Zone privacy reduces visibility



Resolvers

- How many validate?
- Google DNS: Yes
  - DNSSEC signed zones validated unless CD flag set
- OpenDNS: Not yet
- Total requests: ~12% validate DNSSEC (APNIC, 2014)

Resolvers (http://stats.labs.apnic.net/dnssec)



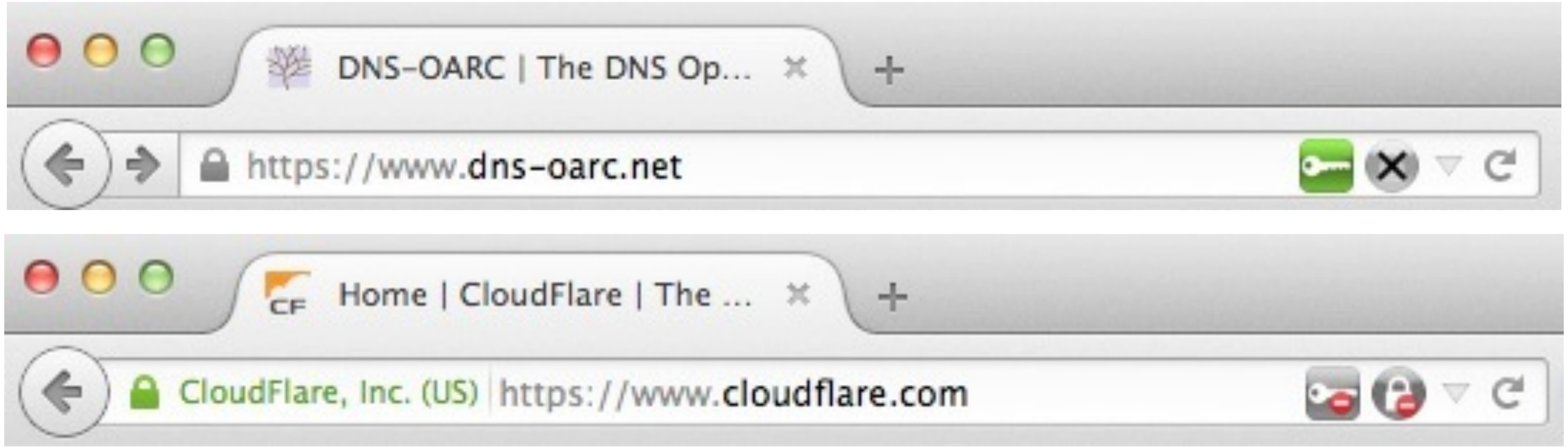
CLOUDFLARE

Registrars

- 30-35 registrars
    - https://www.icann.org/resources/pages/deployment-2012-02-25-en
    - Largest registrar (GoDaddy) supports DNSSEC
- Many require manual email of DS
- Many do not support Elliptic Curve DNSKEYs

Browsers

- No current browser support (was removed from Chrome)
- Plug-in: DNSSEC validator (www.dnssec-validator.cz)



Requirements to work

- Trust chain established (mostly)
- Domains need to be trusted (not many)
- Resolvers need to check (some)
- Users have to be alerted (incomplete)

Where are we going with DNSSEC

Where are we tomorrow?

Slowly happening

- CloudFlare enabling DNSSEC by end of year
- Internet Society's Deploy 360 is tracking deployment

- Continuing research
- Future is yet to be determined

September 24, 2014

DNSSEC: How far have we come?

Nick Sullivan
@grittygrease