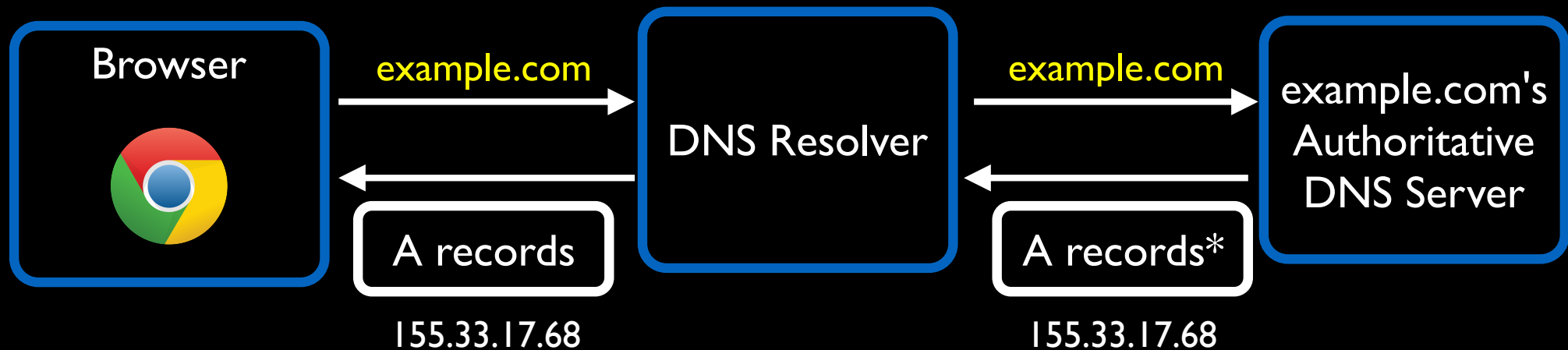


CSCI-759

**Topics In Systems: Public Key
Infrastructure and Network Security**

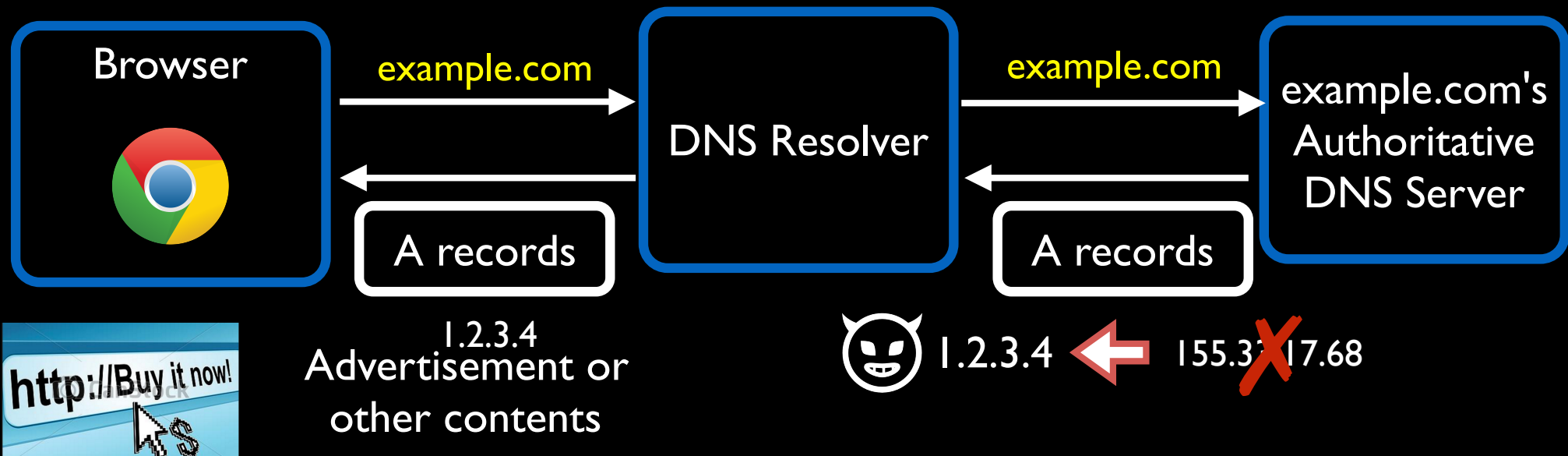
Lecture 2: PKI + DNSSEC

Domain Name System (DNS)

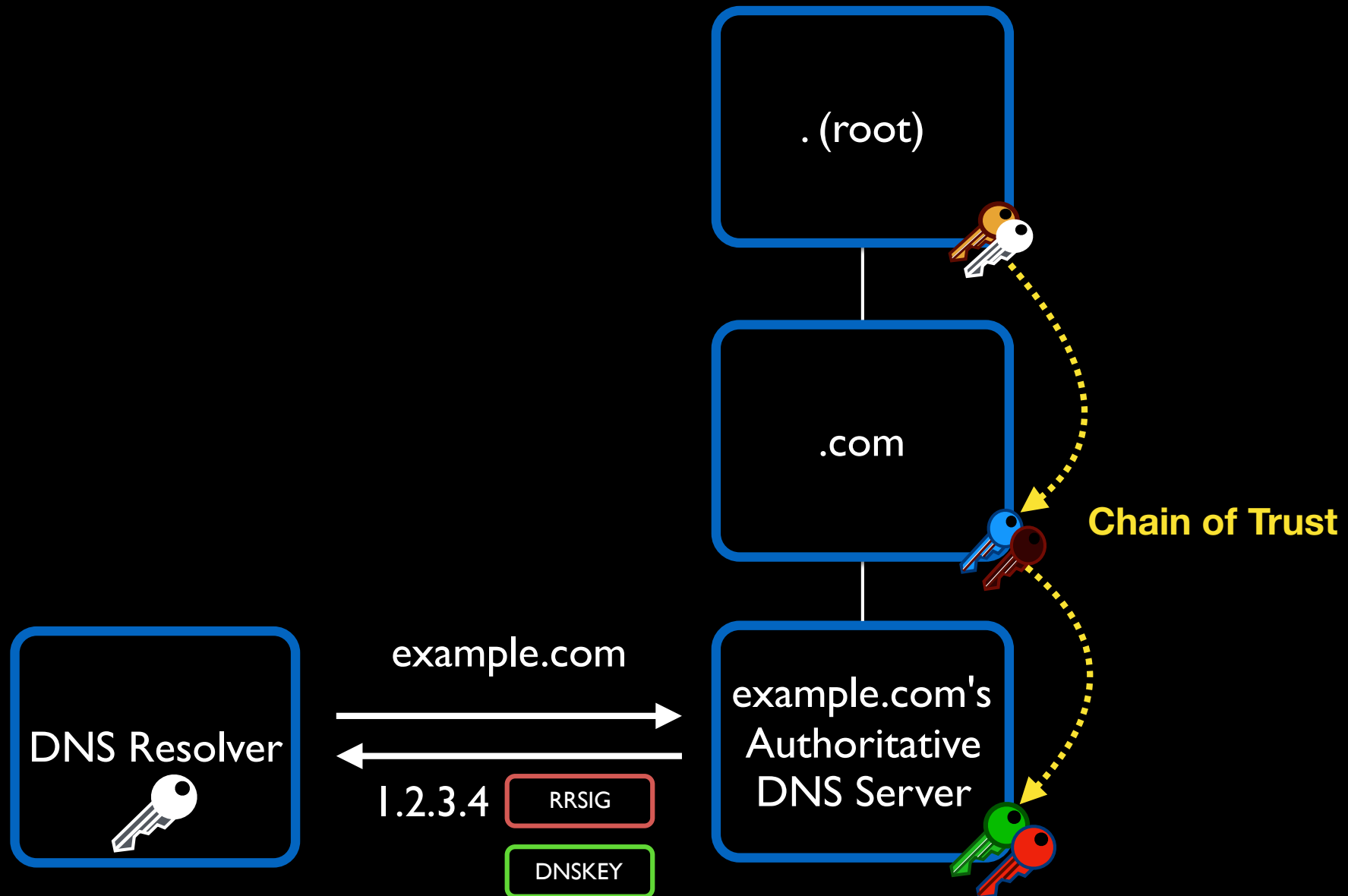


*A record: one of the DNS records that contains IP addresses of a domain name

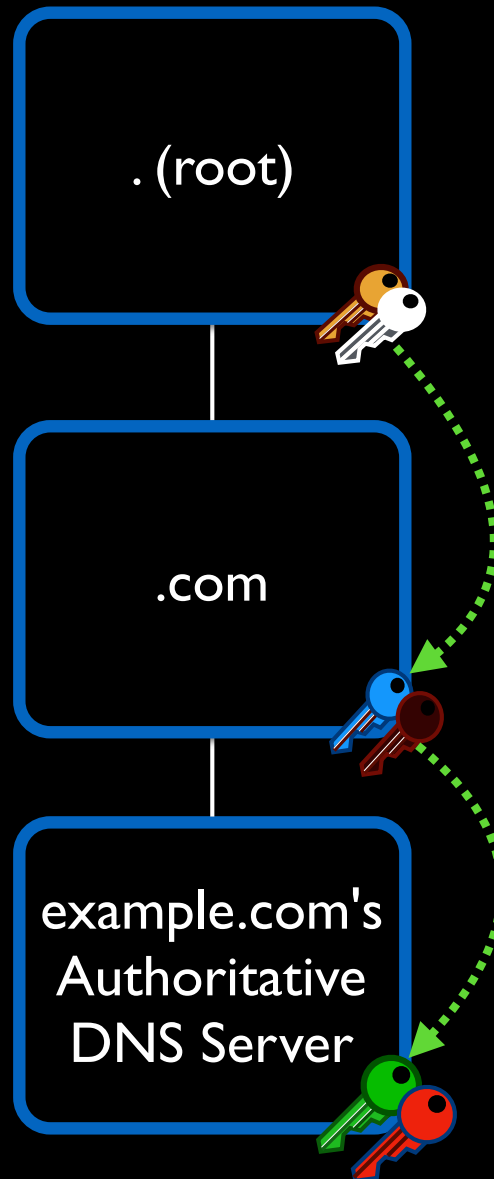
DNS Spoofing



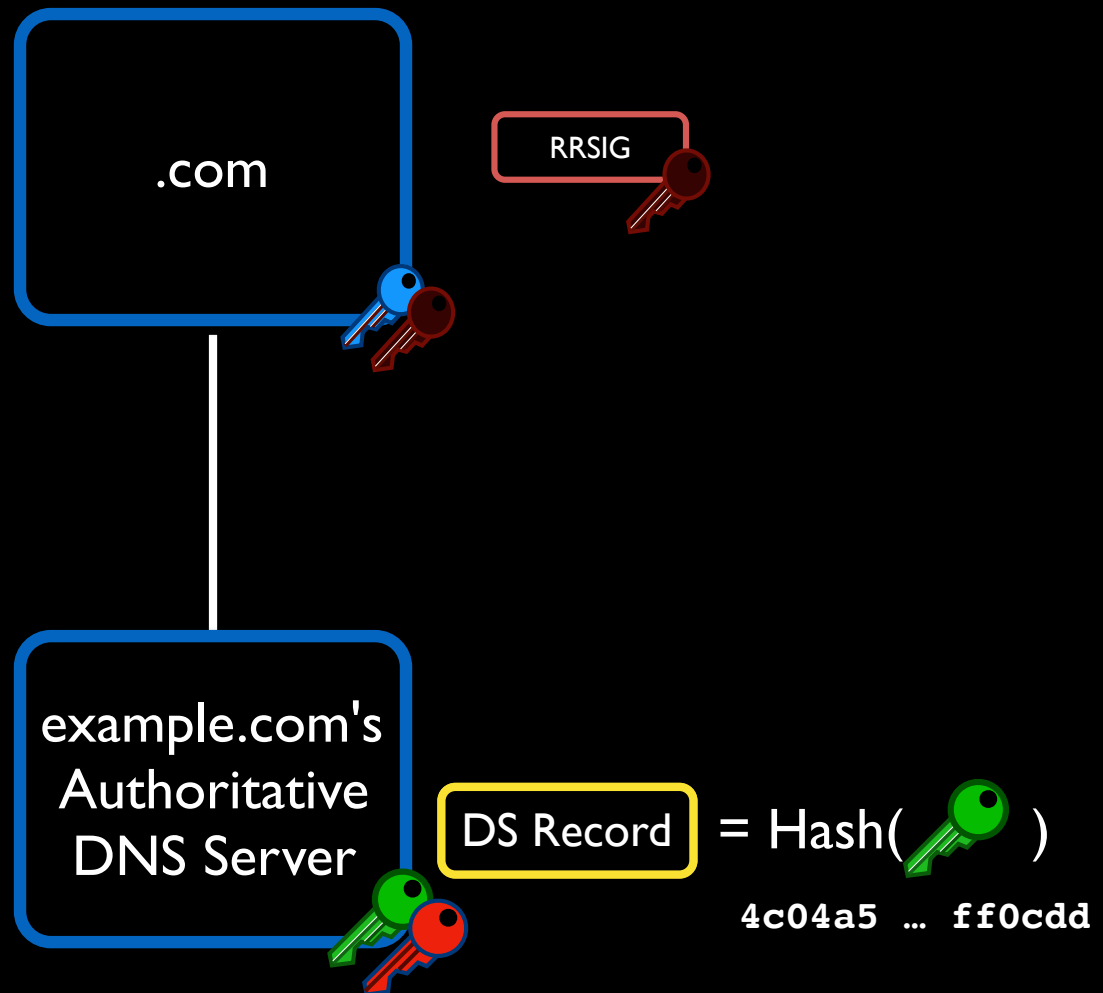
DNSSEC 101



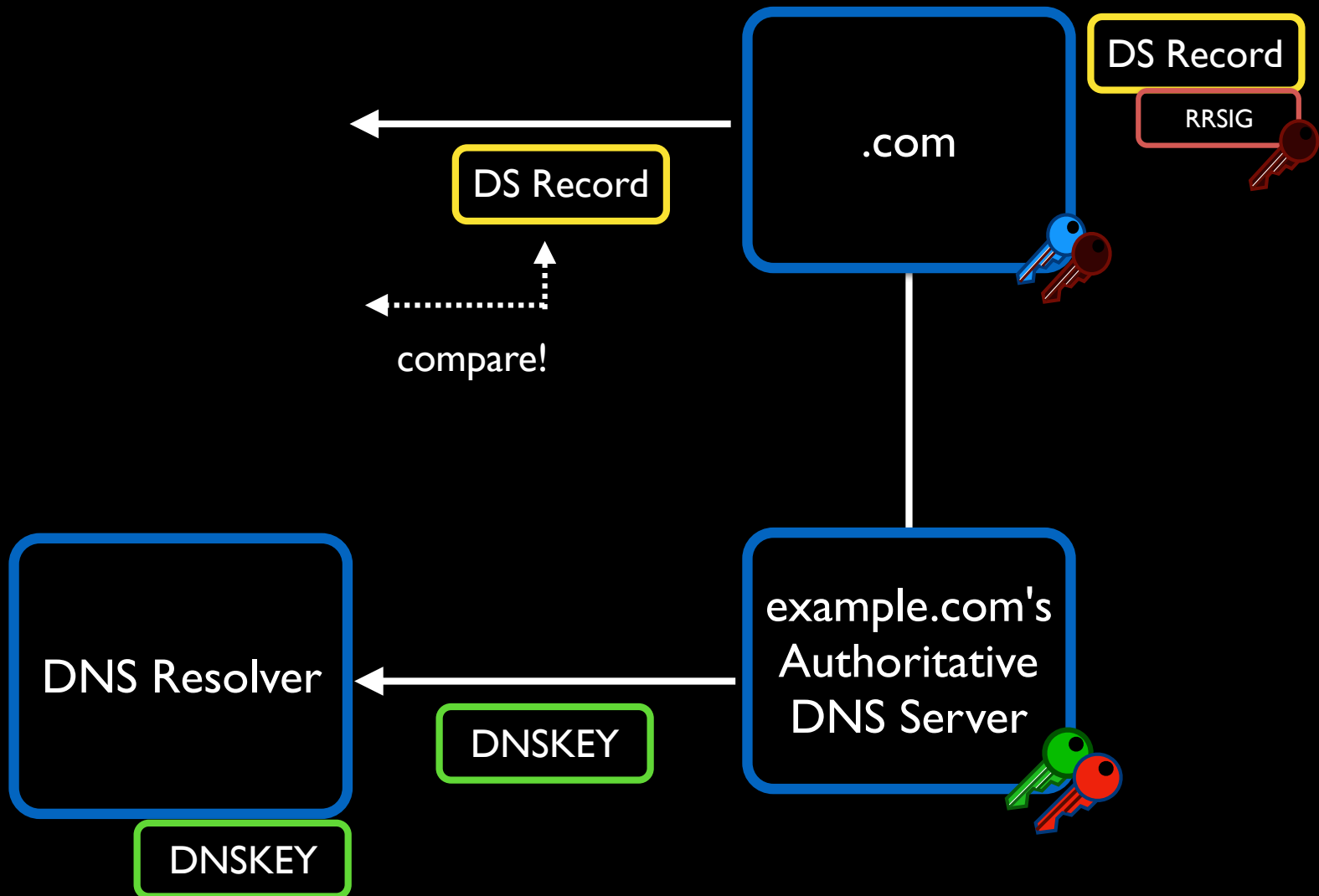
DNSSEC 101



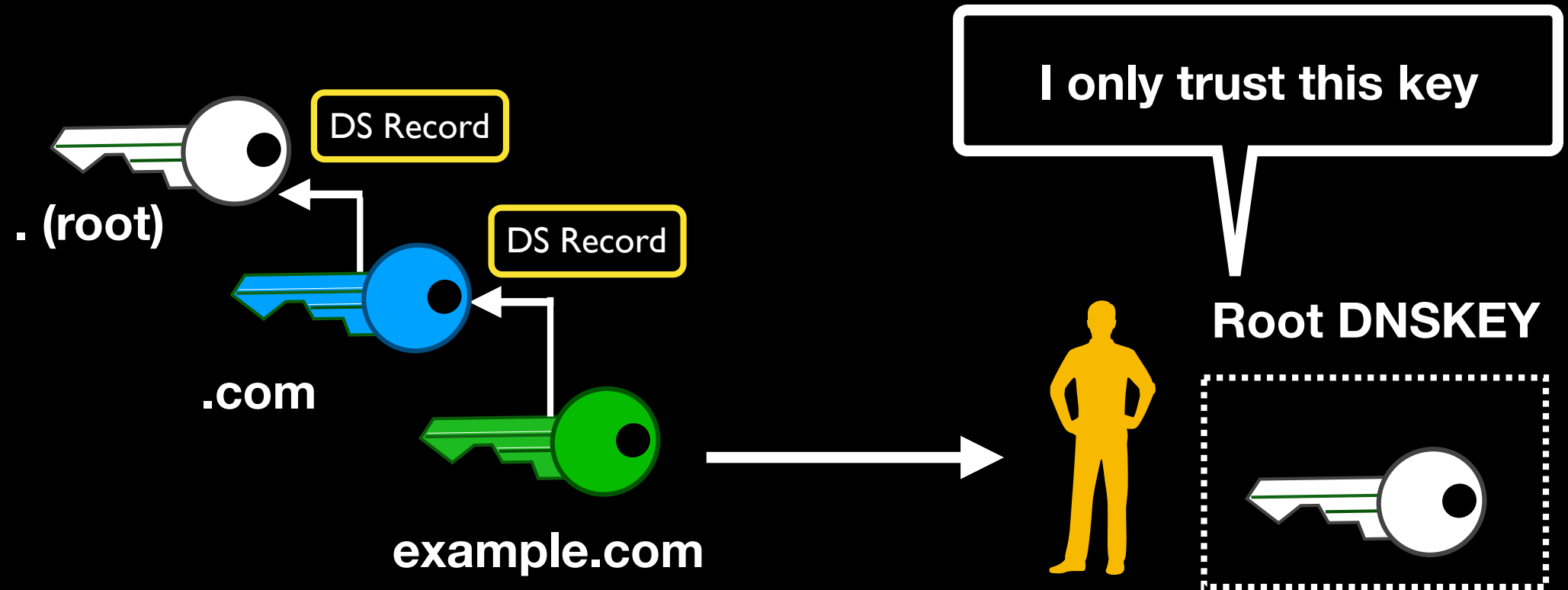
DNSSEC 101: Hierarchy Builds Trust



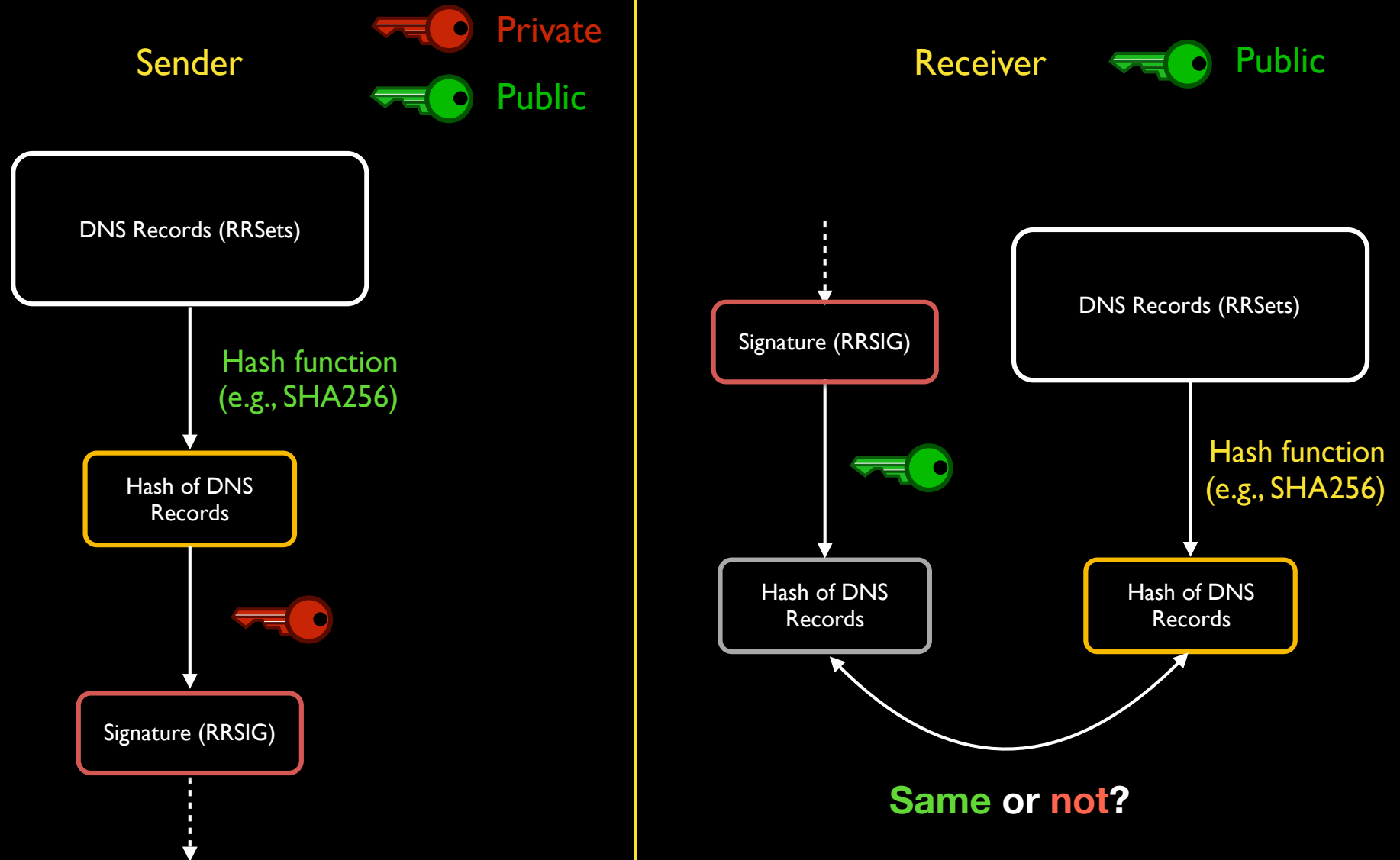
DNSSEC 101: Hierarchy Builds Trust



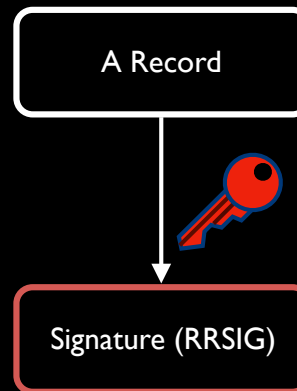
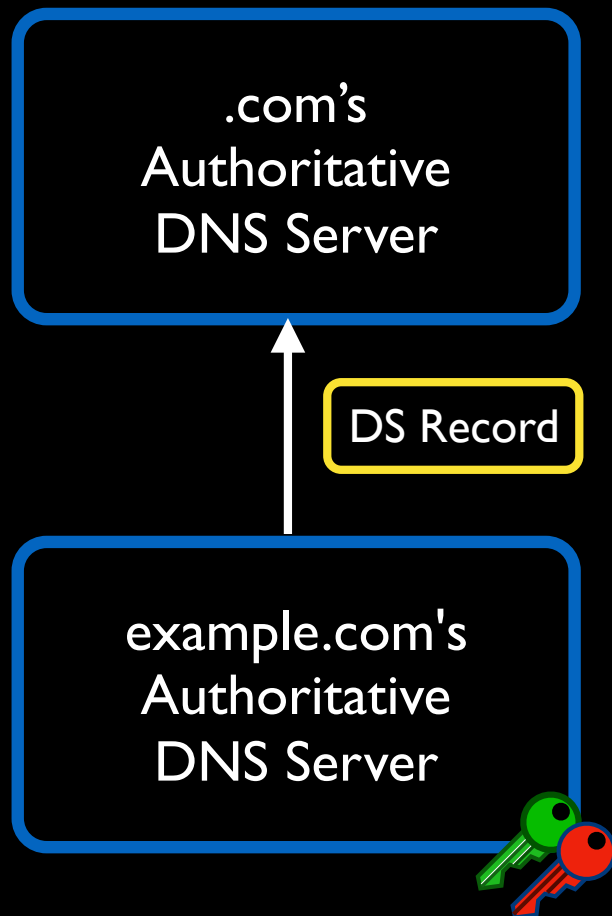
DNSSEC: Hierarchical PKI



Signing and verification process in DNSSEC



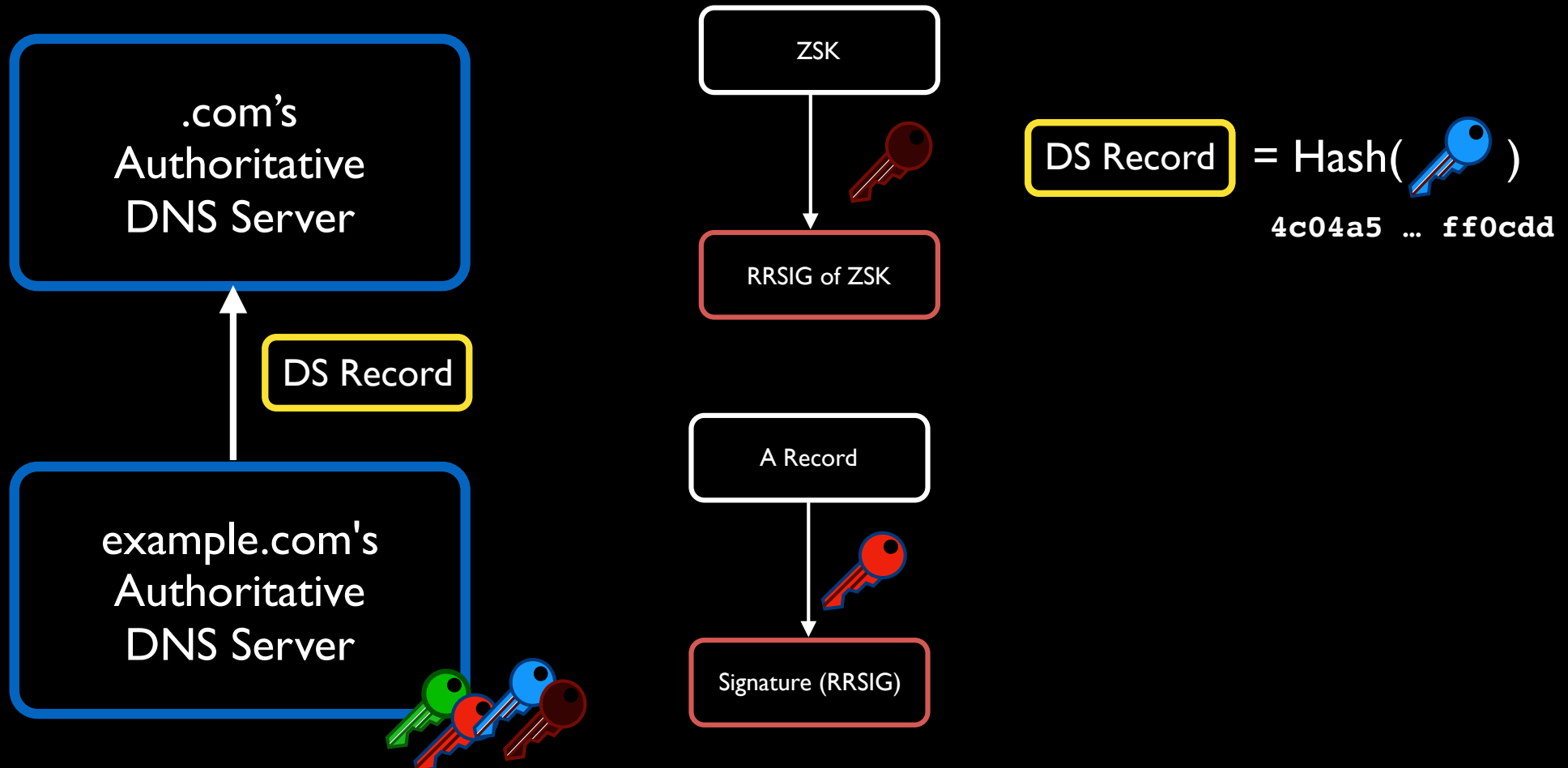
Two DNSKEYs



$$\text{DS Record} = \text{Hash}(\text{key})$$

4c04a5 ... ff0cdd

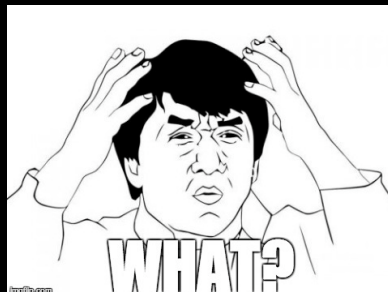
Two DNSKEYs



Key Signing Key (KSK)



Zone Signing Key (ZSK)



Two DNSKEYs

Are you serious? Why?

example.com's
Authoritative
DNS Server



Key Signing Key (KSK)



Zone Signing Key (ZSK)

Only used to generate the
signature of "ZSK"
=> Not heavily used
=> Stored in the offline storage
(e.g., HSM)
=> **More secure!**

Frequently used to
generate signatures for the DNS
records
=> should be loaded on the memory
=> **Not secure**

Revisiting

3 Principles of Information Security

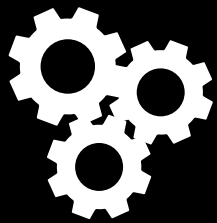
- Confidentiality
- Integrity
- Availability

Motivation of this research



Even though DNSSEC was introduced 20 years ago!

Research Questions



How **well** is today's DNSSEC PKI ecosystem **managed**?

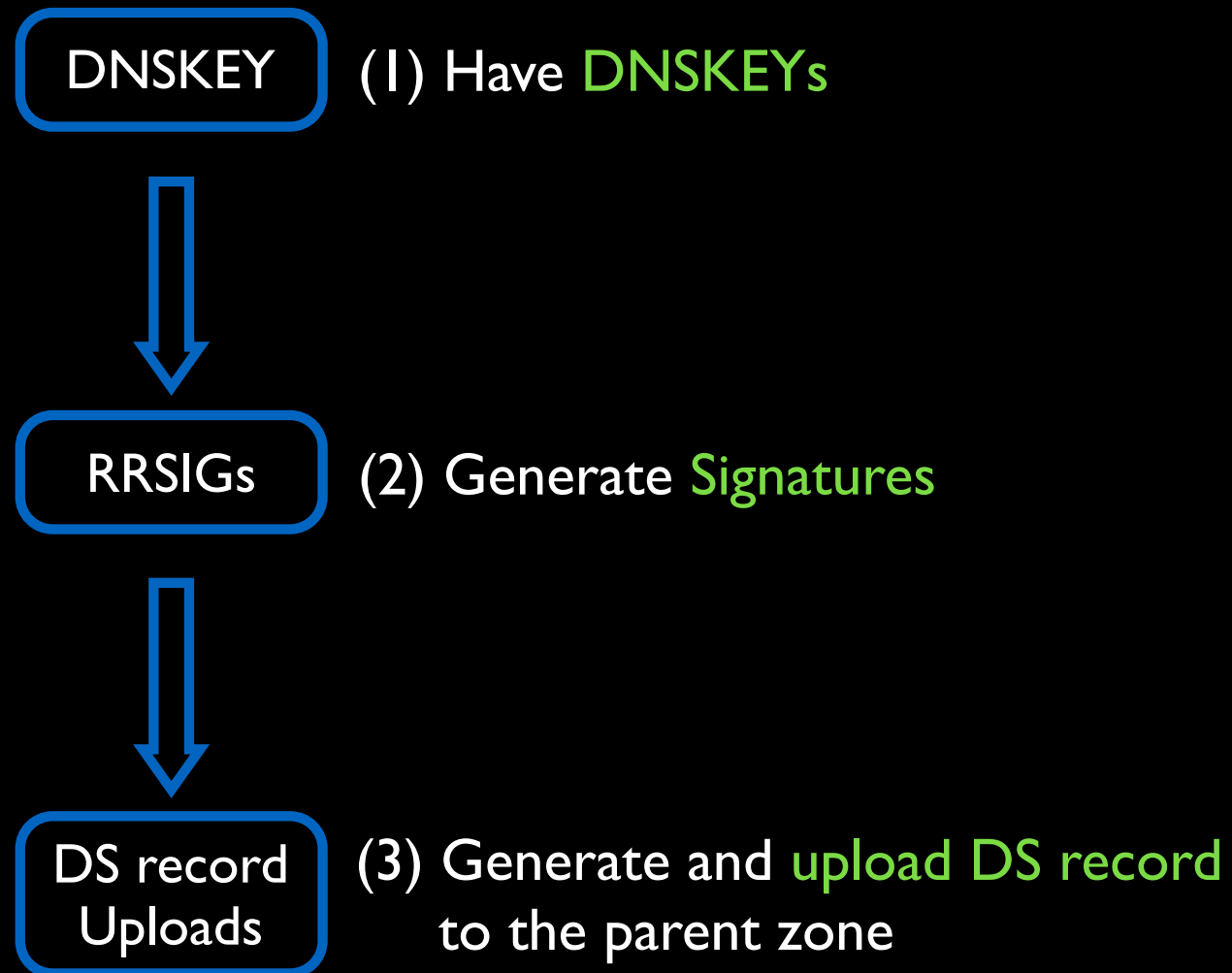


If it is **not** managed well, then **why**?



How can we **improve** it?

How to Deploy DNSSEC (Correctly)



Scanning All Domains

	Daily Scans
TLDs	.com, .org., .net
# of domains	147M domains
Interval	every day
Period	2015/03/01 ~ 2016/12/31

Over 750 billion DNS Records

How DNSSEC is deployed

DNSKEY

~1.0%

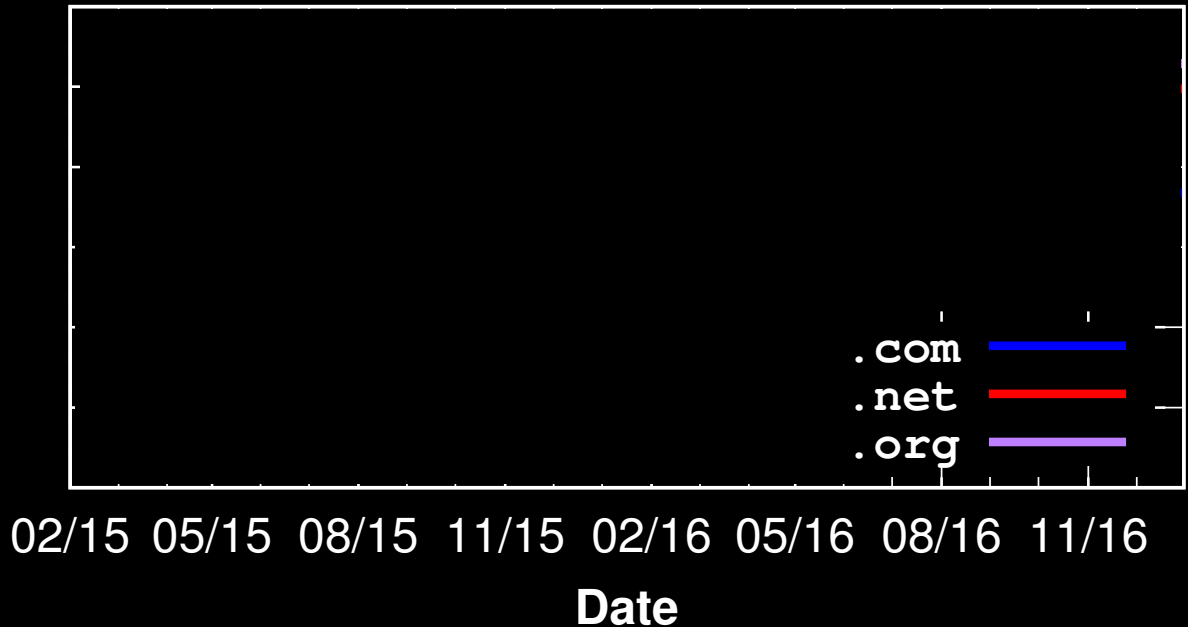


RRSIGs



DS record
Uploads

Percent of domains with
DNSKEY record



Deployment

DNSSEC deployment is rare, but growing

Generating Signatures

DNSKEY

~1.0%



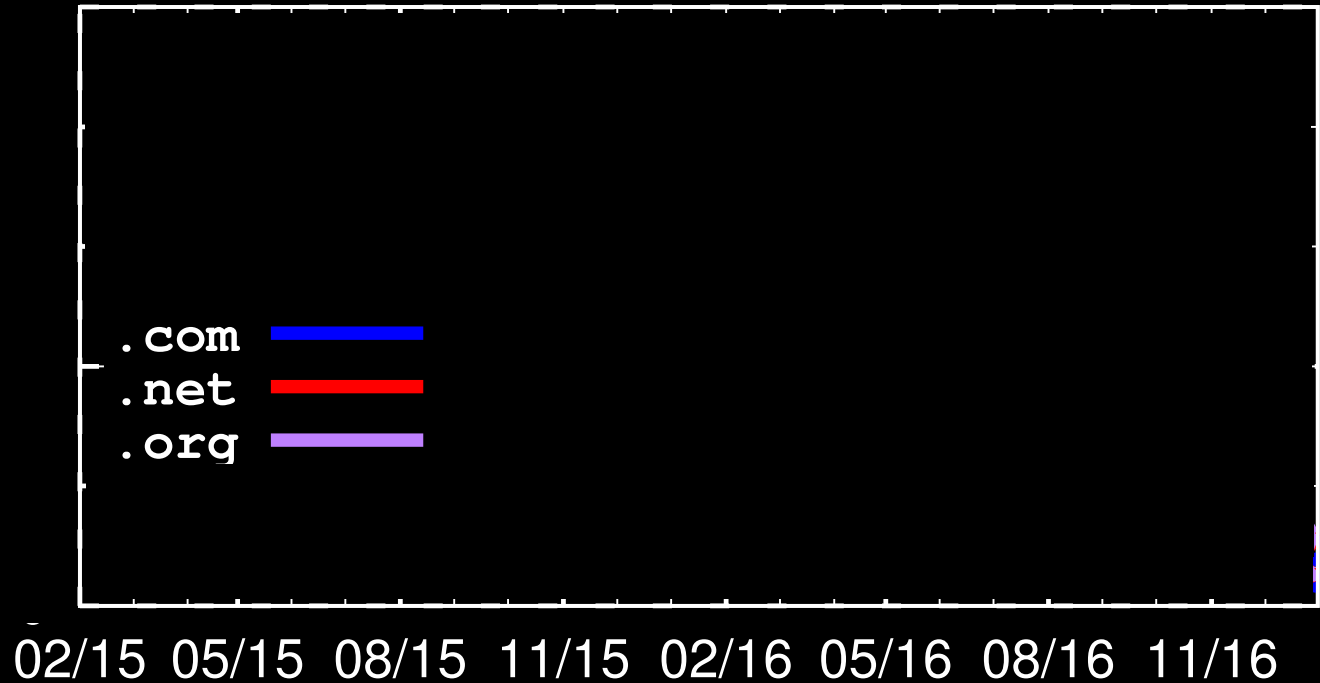
RRSIGs

~0.3%



DS record
Uploads

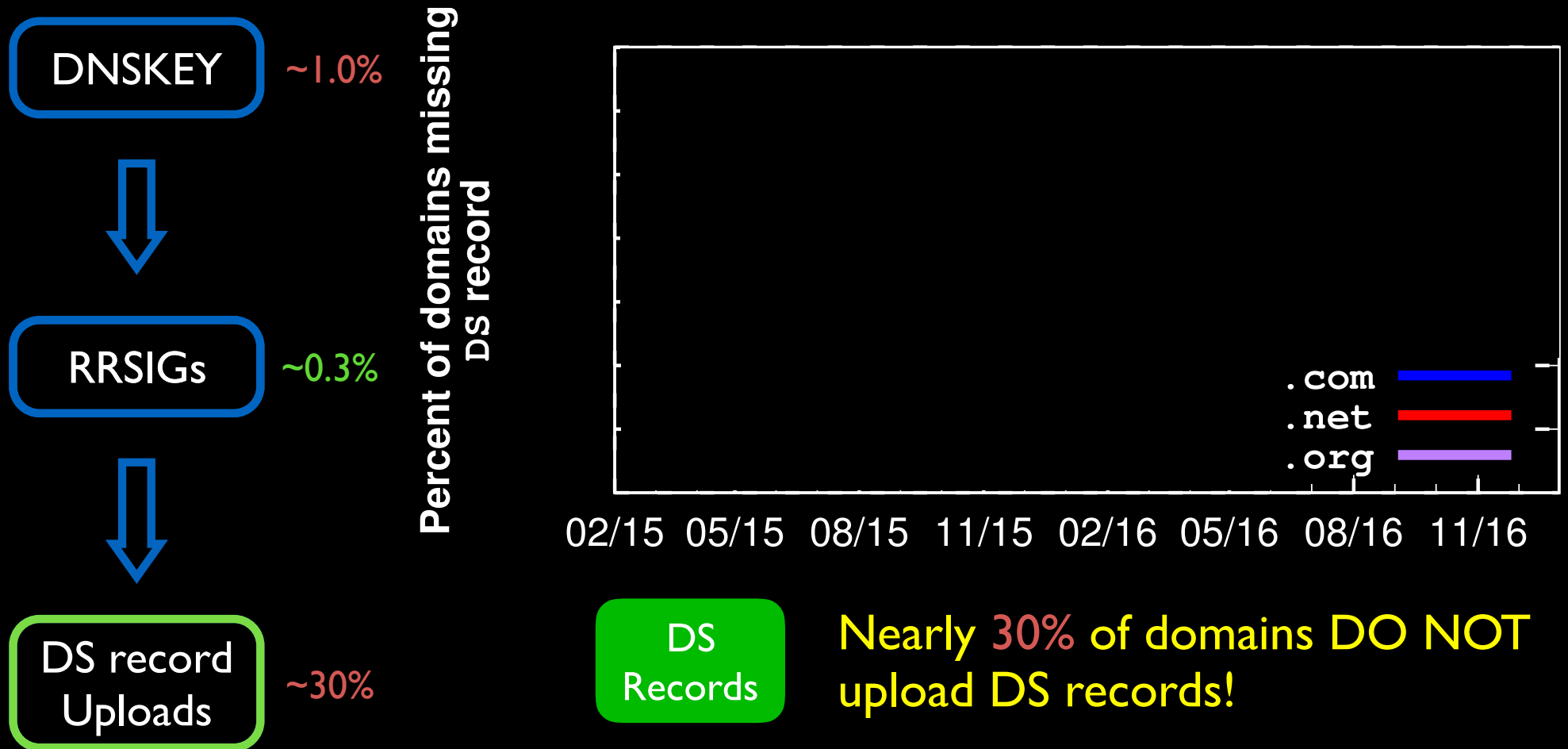
Percent of domains
missing RRSIGs



Missing
RRSIGs

RRSIGs are rarely missing (0.3%)

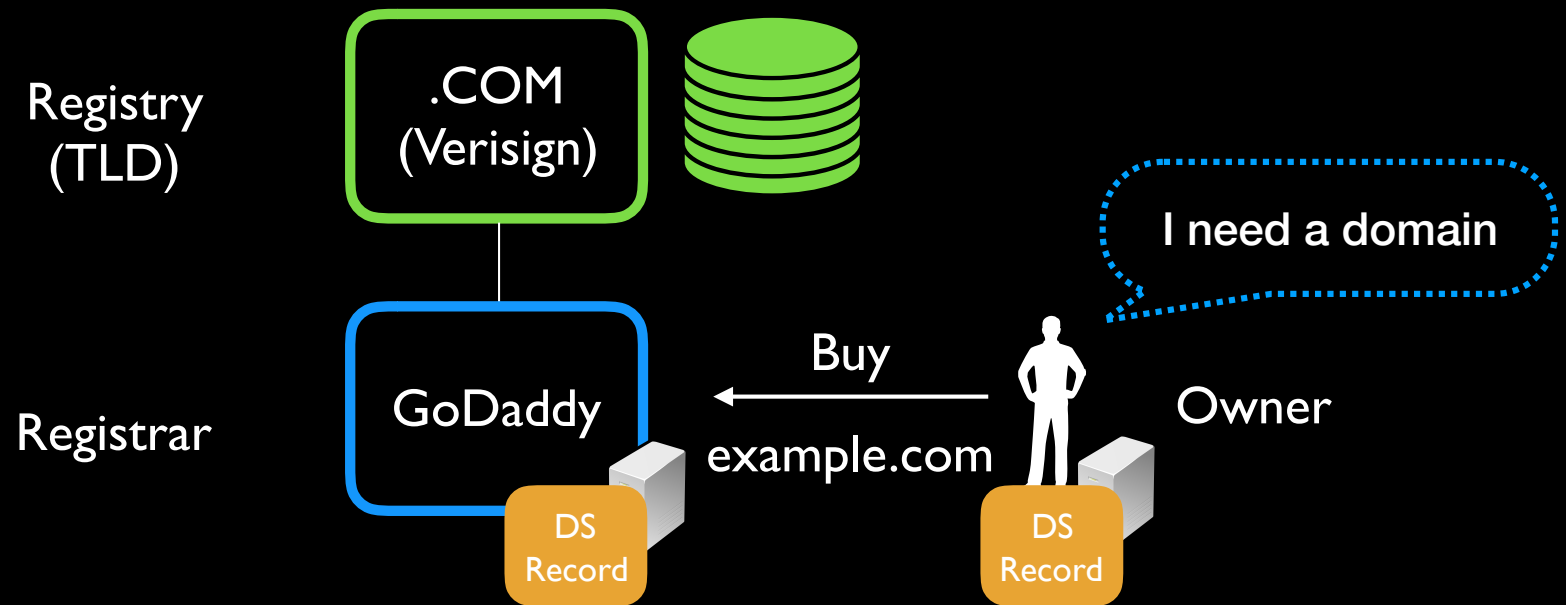
Building a Chain of Trust



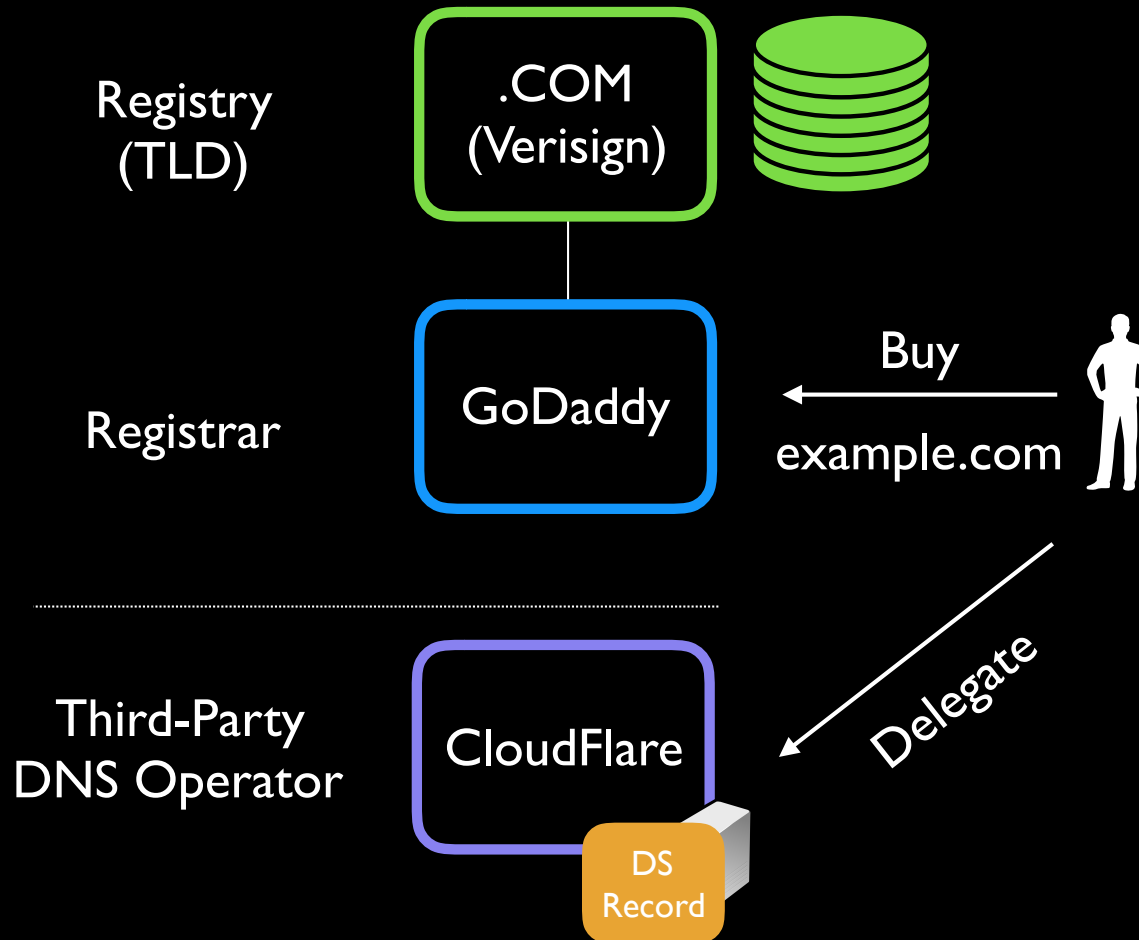
Why does DNSSEC deployment remain so small?

Why are 30% of domains w/o DS records?

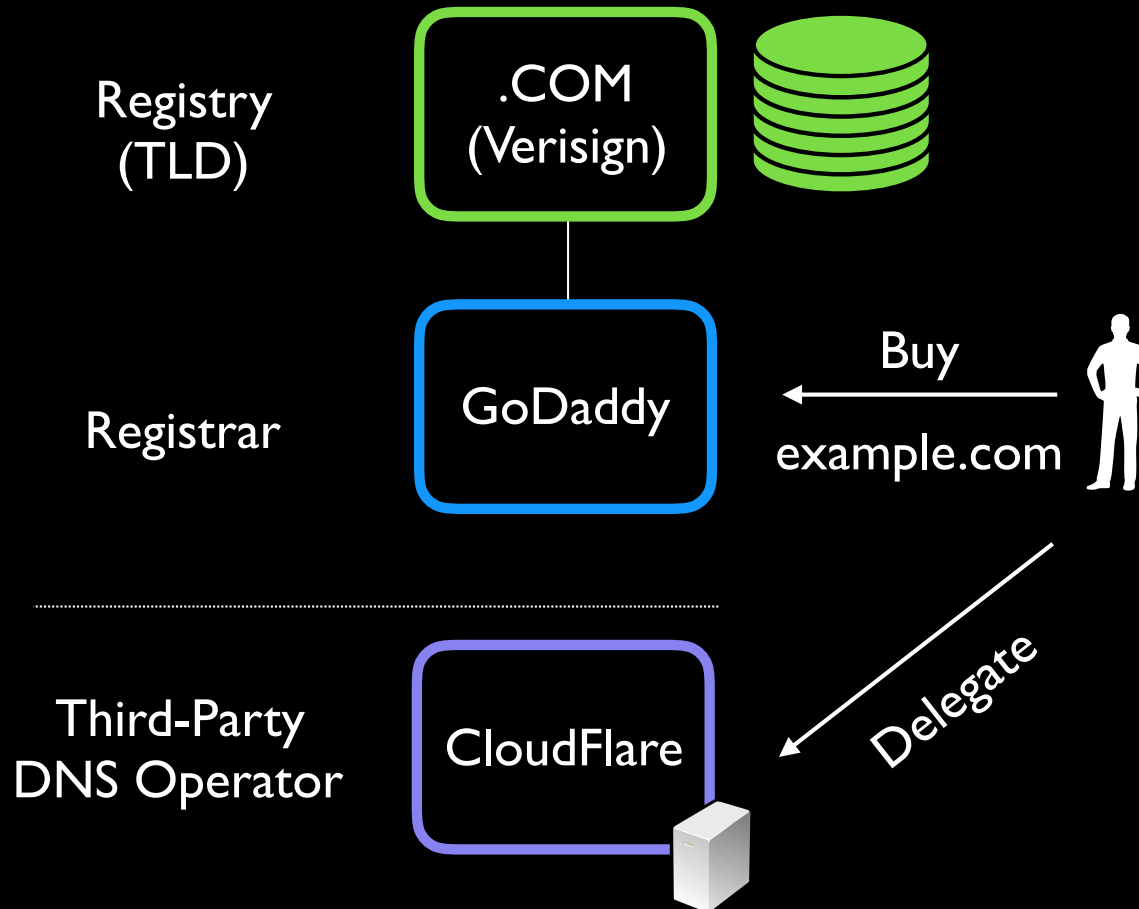
Deploying a DNSSEC on Your Server



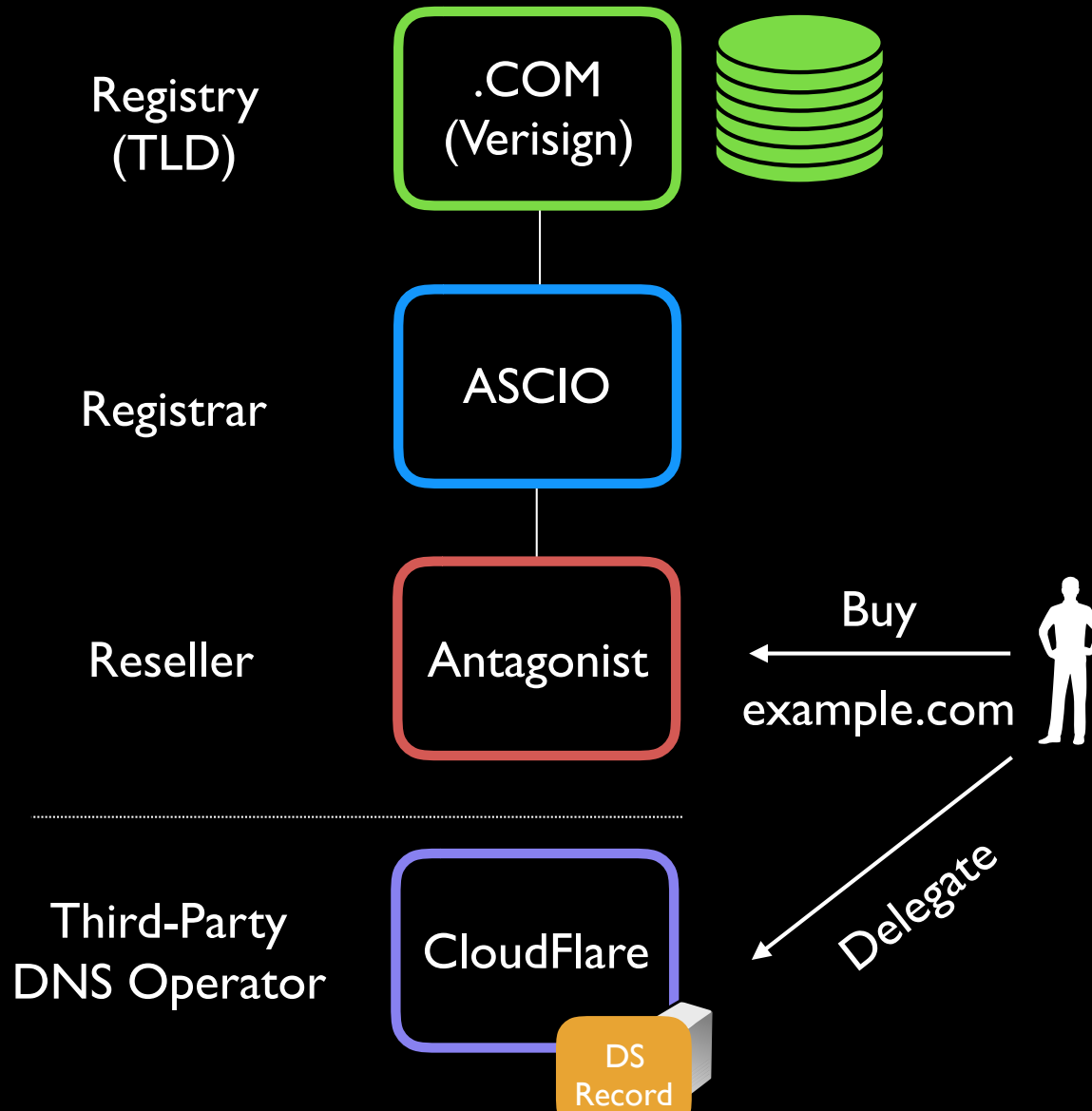
Third Party DNS Operator



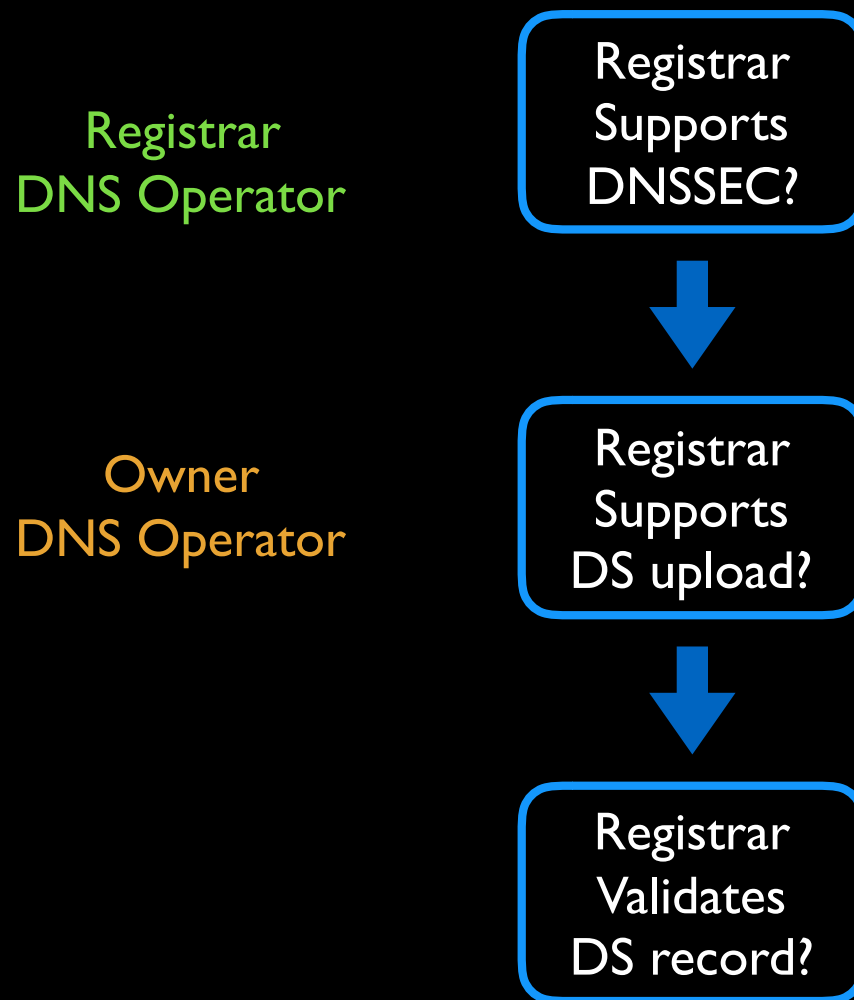
Third Party DNS Operator



Reseller



Checking Registrar's DNSSEC Policy



Popular Registrar's DNSSEC Policy

3/20

Registrar
Supports
DNSSEC?



Registrar
Supports
DS upload?



Registrar
Validates
DS record?

Registrar (Authoritative Nameserver)	Registrar DNS Operator
GoDaddy (domaincontrol.com)	
NameCheap (registrar-servers.com)	
OVH (ovh.net)	
HostGator (hostgator.com)	
Amazon (aws-dns)	
Google (googledomains.com)	
123-reg (123-reg.co.uk)	
RightSide (name.com)	
eNom (name-services.com)	
NameBright (namebrightdns.com)	
DreamHost (dreamhost.com)	
The others (10 registrars)	

Some nameservers don't support DNSSEC

Anecdotal Examples

Experiment

We saw the DNSKEY deployed (but not DS records) so asked why you don't upload DS records.

We asked a registrar to upload a DS record by email from the different email address than the one that registered

We asked a registrar to upload a DS record to our domain via web live chat

Result

[1] They removed a DNSSEC menu

[2] *“Most people do not understand DNS, so imagine the white faces when I mention DNSSEC”*

It was installed successfully

It was installed on *someone else's* domain due to a mistake by the customer service agent

Details of the Last Example

3:45:32 PM **tijay** hg-dnssec.com 3600 IN DS 2371 13 2
129f34c04ac58ece5218b9894148304a736a63757f58ff0cddd9b8df4989

3:56:05 PM **Jeniffer S** Awesome! one moment

3:56:09 PM **Jeniffer S** I have now save the request
information! Manage DNSSEC **paananenmusic.com** Record added
successfully. It can take 4-8 hours for DNS to propagate

3:57:19 PM **tijay** paananenmusic.com?

3:57:28 PM **tijay** my domain is hg-dnssec.com?

3:58:41 PM **Jeniffer S** I apologize, you are right, silly me,
one moment

Popular Registrar's DNSSEC Policy

3/20

Registrar
Supports
DNSSEC?



11/20

Registrar
Supports
DS upload?



Registrar
Validates
DS record?

Registrar (Authoritative Nameserver)	Owner DNS Operator	
	DS Upload	
	Web	Email
GoDaddy (domaincontrol.com)	●	—
NameCheap (registrar-servers.com)	●	—
OVH (ovh.net)	●	—
HostGator (hostgator.com)	●	—
Amazon (aws-dns)	●	—
Google (googledomains.com)	●	—
123-reg (123-reg.co.uk)	●	—
RightSide (name.com)	●	—
eNom (name-services.com)	✗	●
NameBright (namebrightdns.com)	✗	●
DreamHost (dreamhost.com)	✗	●
The others (10 registrars)	✗	✗

Popular Registrar's DNSSEC Policy



Registrar (Authoritative Nameserver)	Owner DNS Operator		DS Validation
	DS Upload		
	Web	Email	
GoDaddy (domaincontrol.com)	●	—	✗
NameCheap (registrar-servers.com)	●	—	✗
OVH (ovh.net)	●	—	●
HostGator (hostgator.com)	●	—	✗
Amazon (aws-dns)	●	—	✗
Google (googledomains.com)	●	—	✗
123-reg (123-reg.co.uk)	●	—	✗
RightSide (name.com)	●	—	✗
eNom (name-services.com)	✗	●	✗
NameBright (namebrightdns.com)	✗	●	✗
DreamHost (dreamhost.com)	✗	●	●
The others (10 registrars)	✗	✗	✗

Summary: Registrar's DNSSEC Support

	DNS Operator	# of Registrar	What this means to you
Support DNSSEC?	Registrar	3/20	If you don't want to run your own name server, most of the time, you CAN'T deploy DNSSEC (17/20)
	Owner	11/20	If you do want run your own nameserver, still you CAN'T deploy DNSSEC for 9/20
Check DS Validation	Owner	2/11	If you happen to upload an incorrect DS record, your domain will be inaccessible

Why are DNSSEC support of registrars so rare?

Cost of Managements

	DNS	DNSSEC
# of Records	DNSSEC introduces much more records (e.g., need signatures for each record)	
Size of Records	Signatures are usually 3~6 times larger than non-DNSSEC records*	
Management	-	Strong Key Unique Key Rollover

Operational
Cost

Operational cost of DNSSEC is higher than
that of DNS

Case Study: Registrar's Policy

	Registrar DNS Operator		Owner DNS Operator	
	Support DNSSEC	Pricing	Support DNSSEC	Pricing
# of registrars	3	Free: 2	11	Free
		Paid: 1		

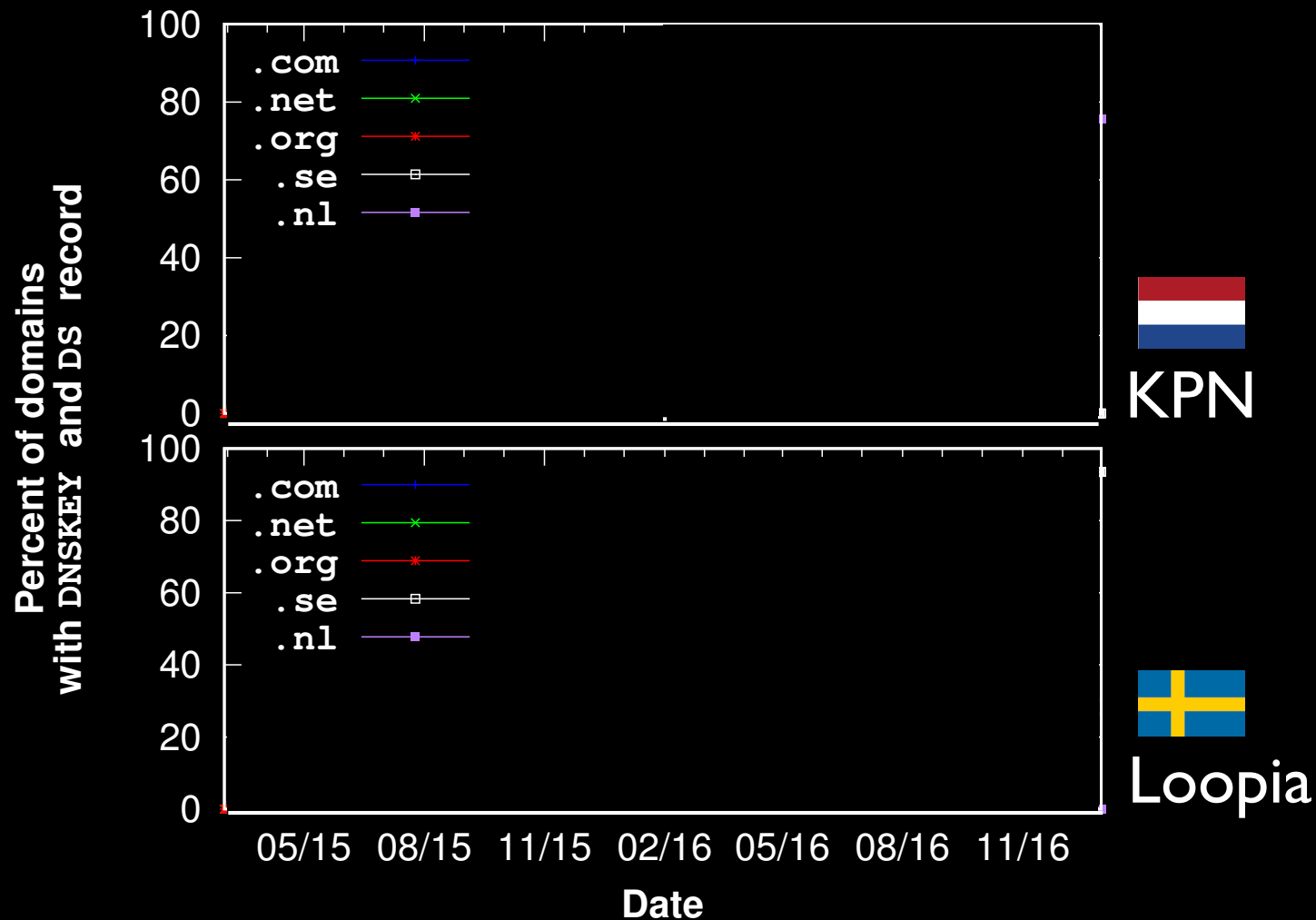
Registrars manage
all DNS records

Registrars DO NOT need to
manage DNS records at all

Scanning All Domains

TLD	Measurement Period (Daily Scan)	Domains	
		Total	Percent w/ DNSKEY
.com	2015/03/01 ~ 2016/12/31	118,147,199	0.7%
.net	2015/03/01 ~ 2016/12/31	13,773,903	1.0%
.org	2015/03/01 ~ 2016/12/31	9,682,750	1.1%
.nl	2016/02/09 ~ 2016/12/31	5,674,208	51.6%
.se	2016/06/07 ~ 2016/12/31	1,388,372	46.7%

Case Study: Financial Incentives

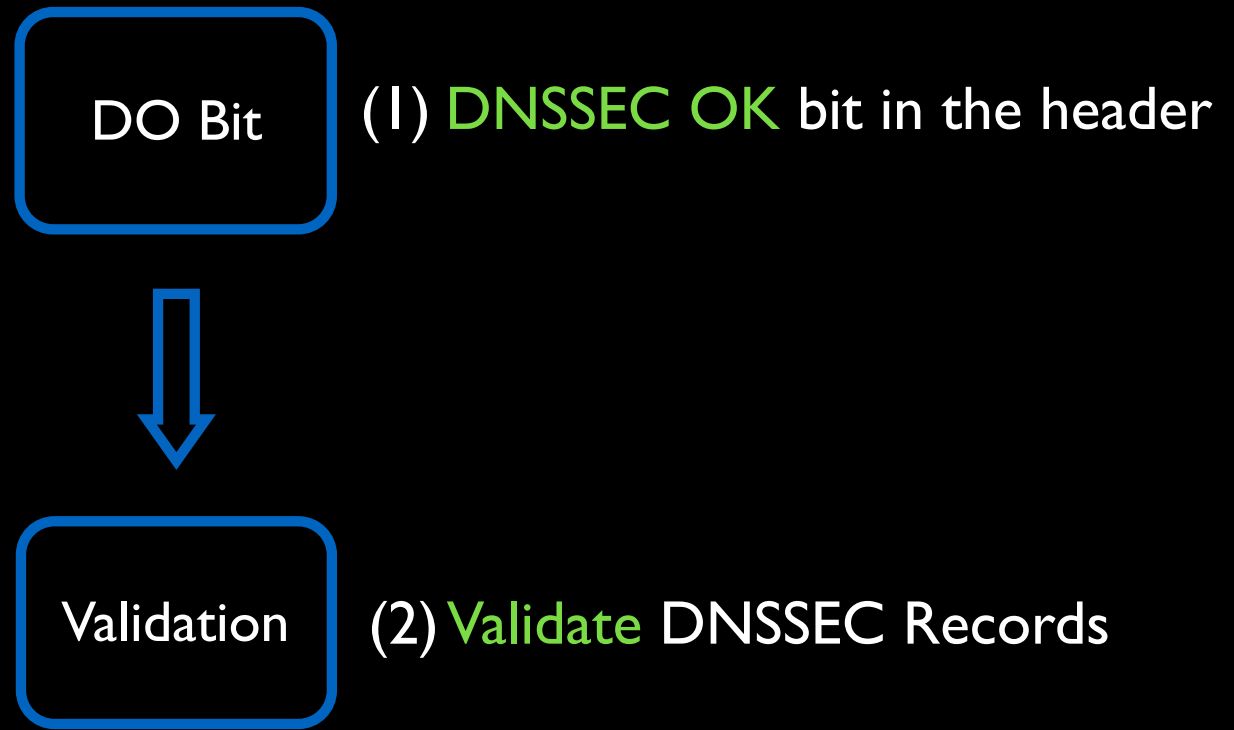


Financial
Incentive

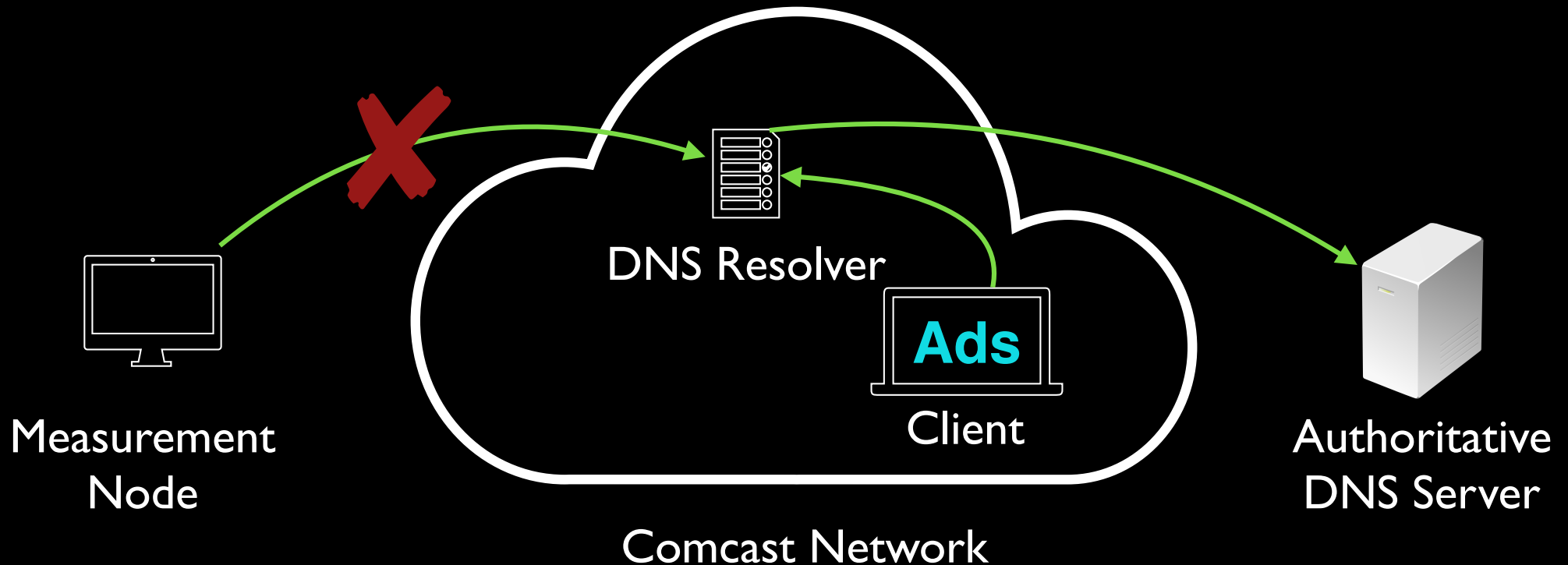
Financial gain is a huge incentive
for deploying DNSSEC to certain domains

DNSSEC Resolvers

Correct Deployment for Resolvers



Measuring DNS resolver



No Control over the node
Not Reproducible



Hola Unblocker



[CDN](#) | [VPN](#) | [AdBlock](#) | [Accelerator](#) | [Browser](#)



[FAQ](#)

[Sign up](#)

Access any website

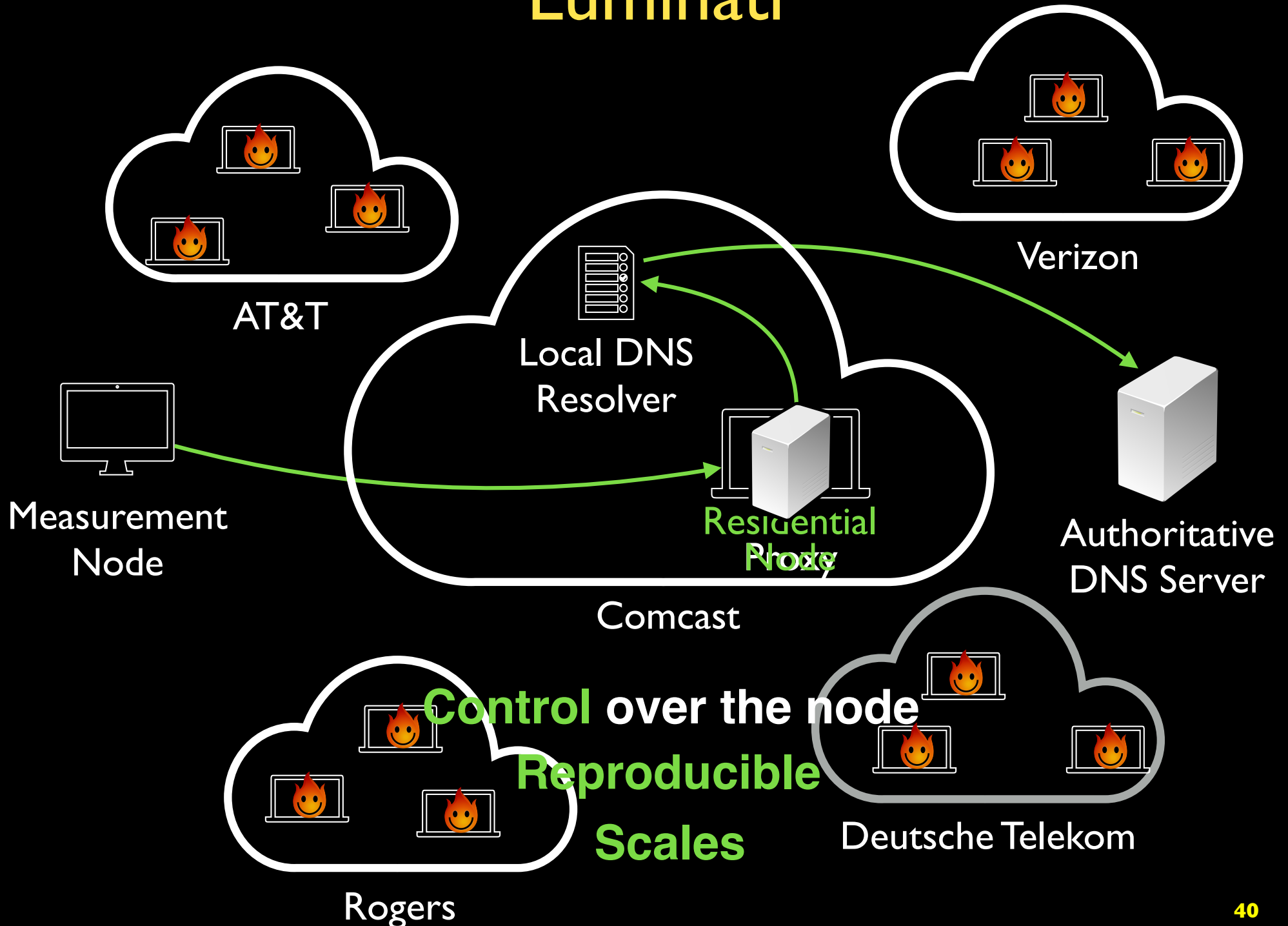
Used by over **95 million** people around the world

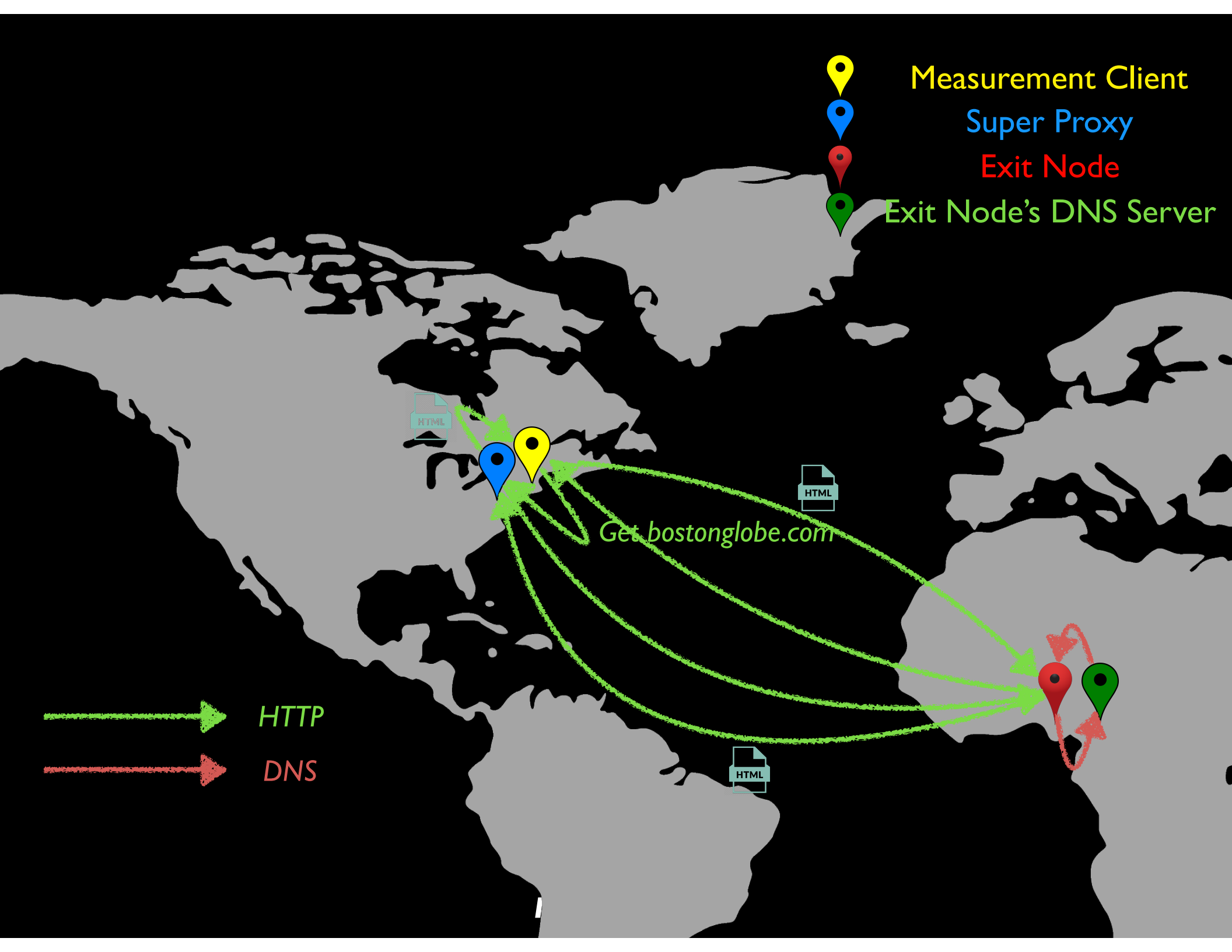
Get Hola **VPN**, it's free!

Start ▶

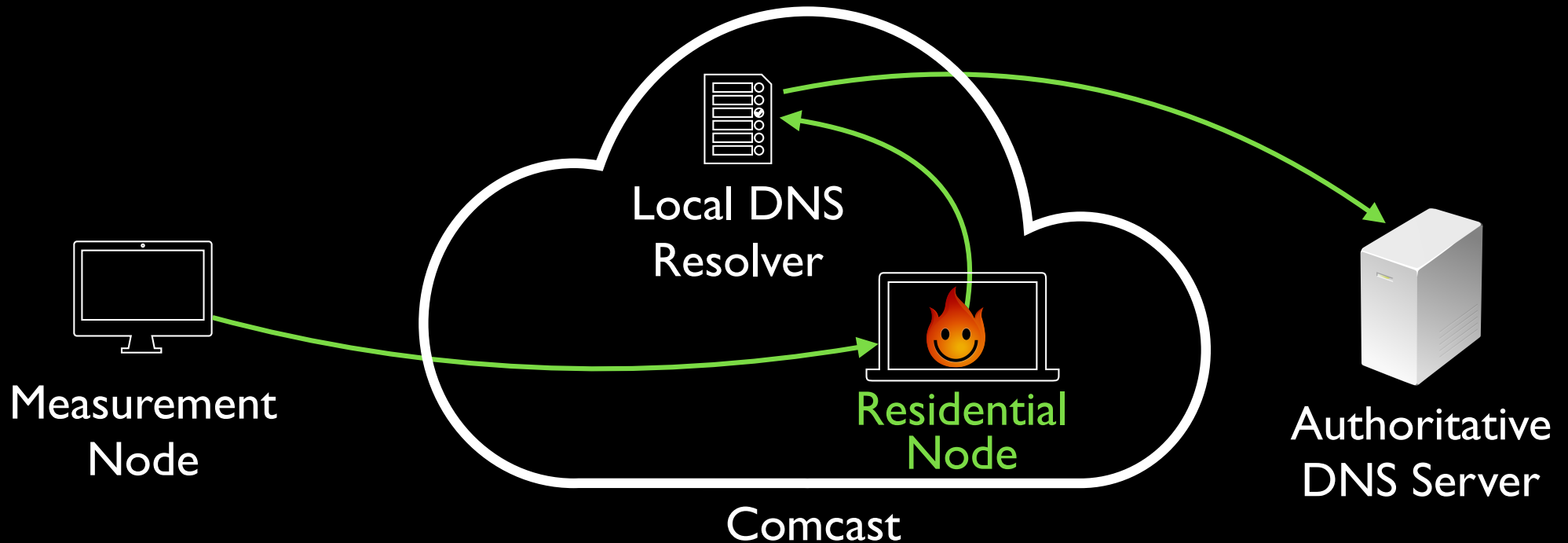
NENS'2016

Luminati





Luminati



Control over the node
Reproducible
Scales

Methodology



+ 8 other scenarios of
incorrect DNSSEC records

Resolvers w/ DO Bit

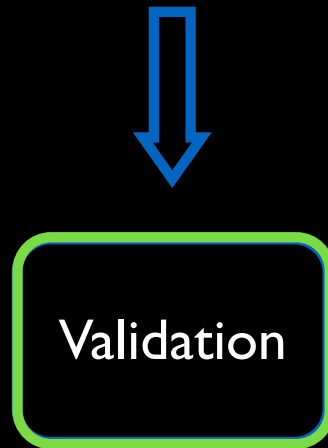
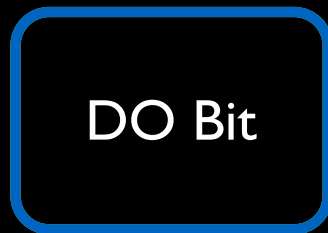
DO Bit

- 4,427 resolvers
- 83% of them are DO-bit enabled



Validation

Resolvers w/ DO Bit



- 4,427 resolvers
- 83% of them are DO-bit enabled
- 3,635 (82%) fail to validate DNSSEC records
 - Time Warner Cable Internet
 - Rogers Cable Communications
- 543 (12.2%) correctly validate DNSSEC records
 - Comcast
 - Google

Open Resolver Tests

Provide	DO Bit	Requested		Validated?
		DS	DNSKEY	
Verisign	YES	YES	YES	YES
Google	YES	YES	YES	YES
DNSWatch	YES	YES	YES	YES
DNS Advantage	YES	YES	YES	YES
Norton ConnectSafe	YES	YES	YES	YES