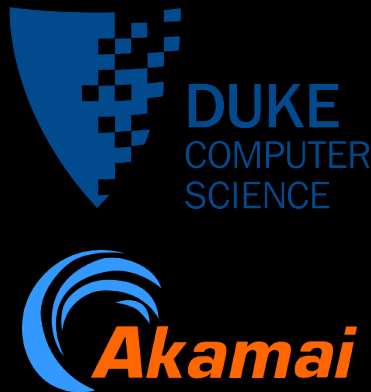# Understanding the Role of Registrars in DNSSEC Deployment [IMC'17]
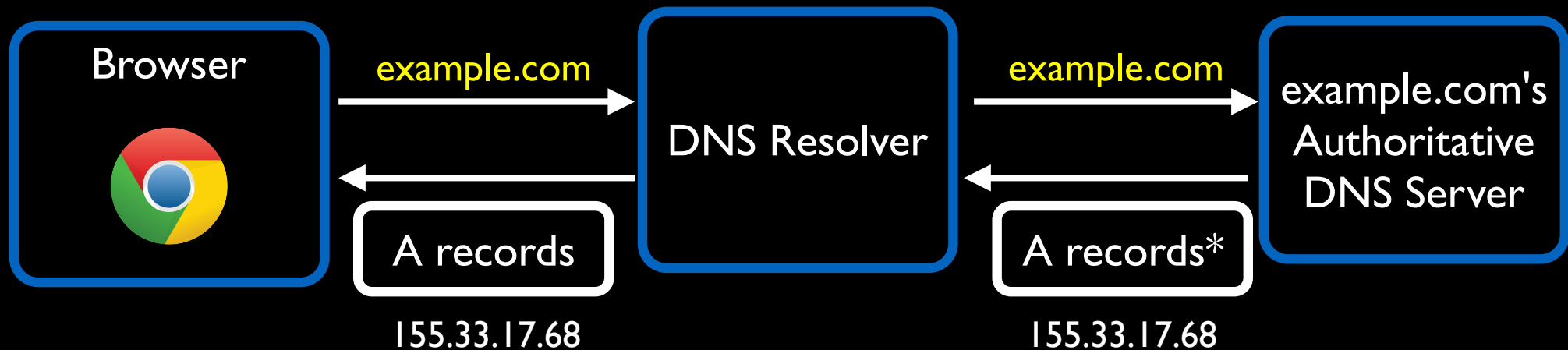
Taejoong (tijay) Chung
Roland van Rijswijk-Deij, David Choffnes,
Dave Levin, Bruce M. Maggs, Alan Mislove, Christo Wilson

1

Domain Name System (DNS)
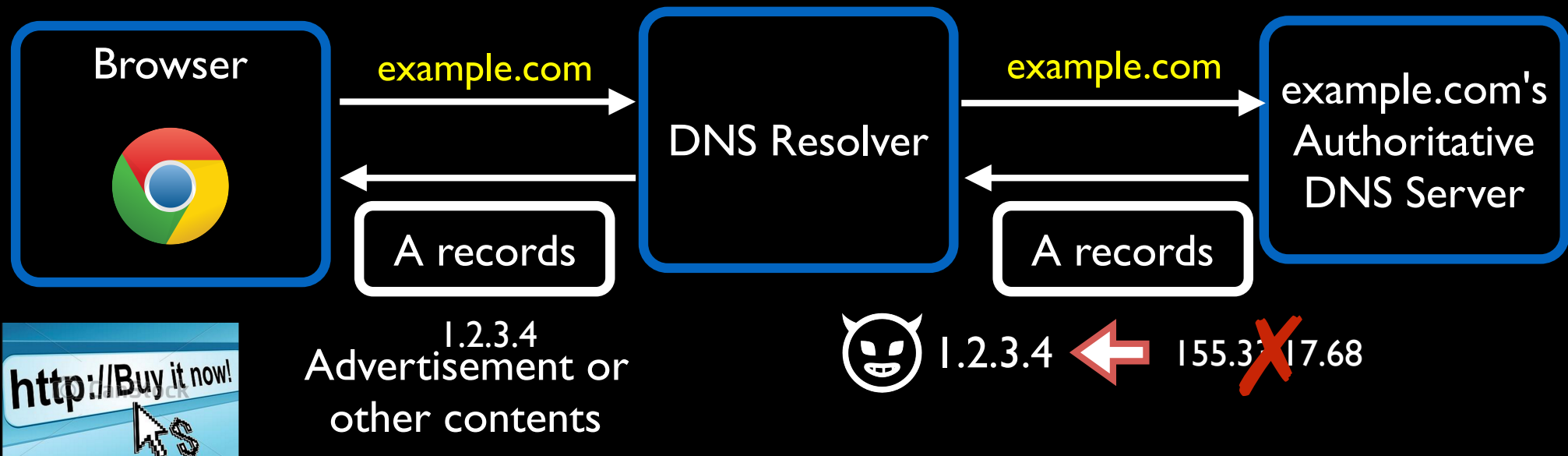

Browser

example.com →

DNS Resolver

example.com →

example.com's Authoritative DNS Server
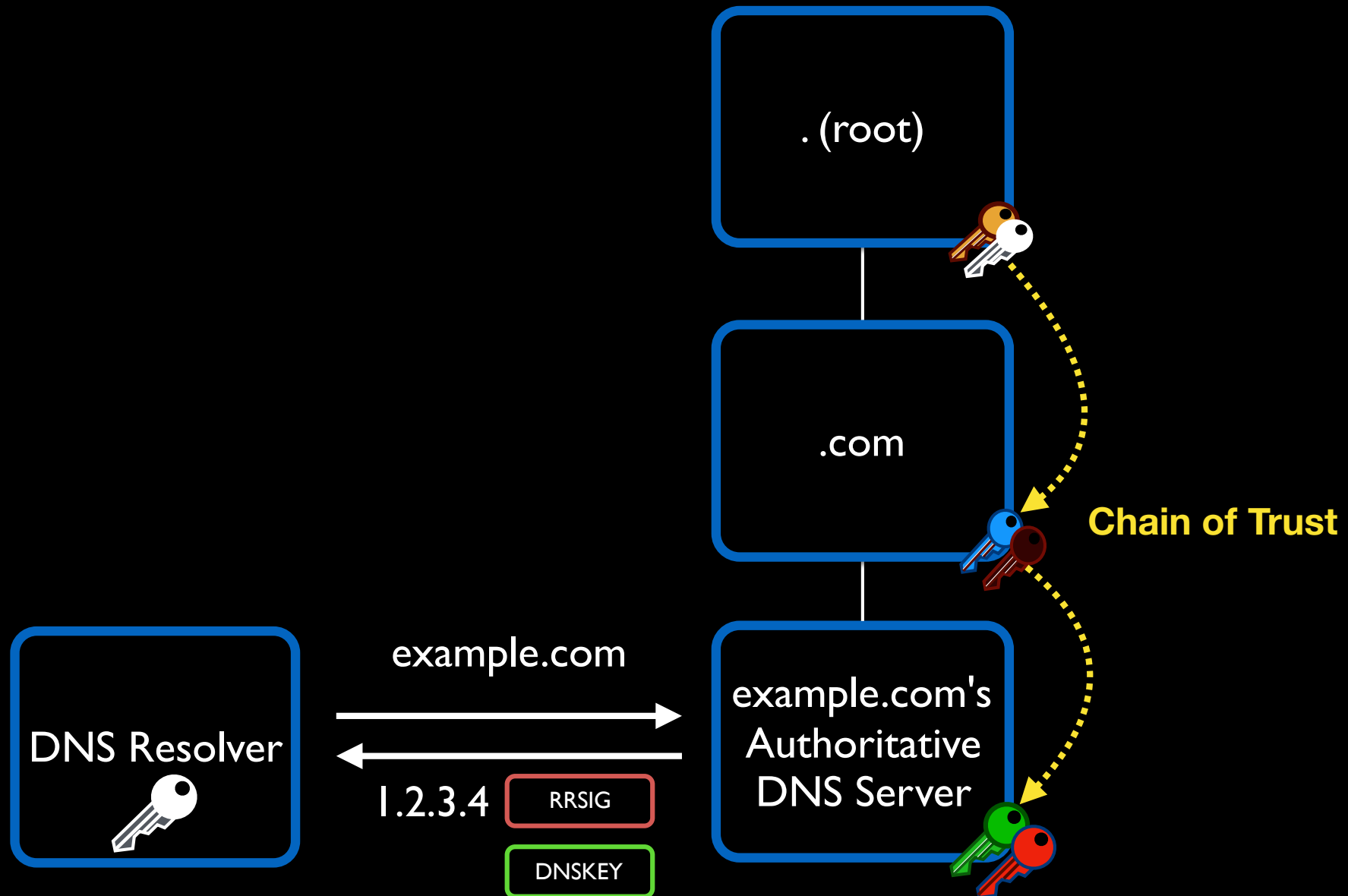
← A records

155.33.17.68

← A records*

155.33.17.68

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

DNS Spoofing

DNSSEC 101

. (root)

.com

Chain of Trust

DNS Resolver

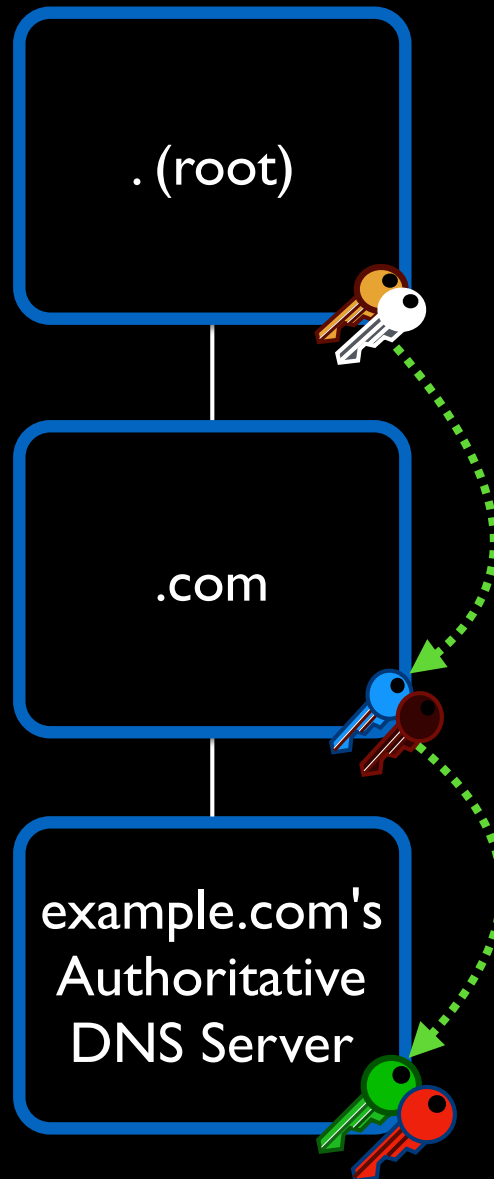example.com

example.com's
Authoritative
DNS Server

1.2.3.4 RRSIG
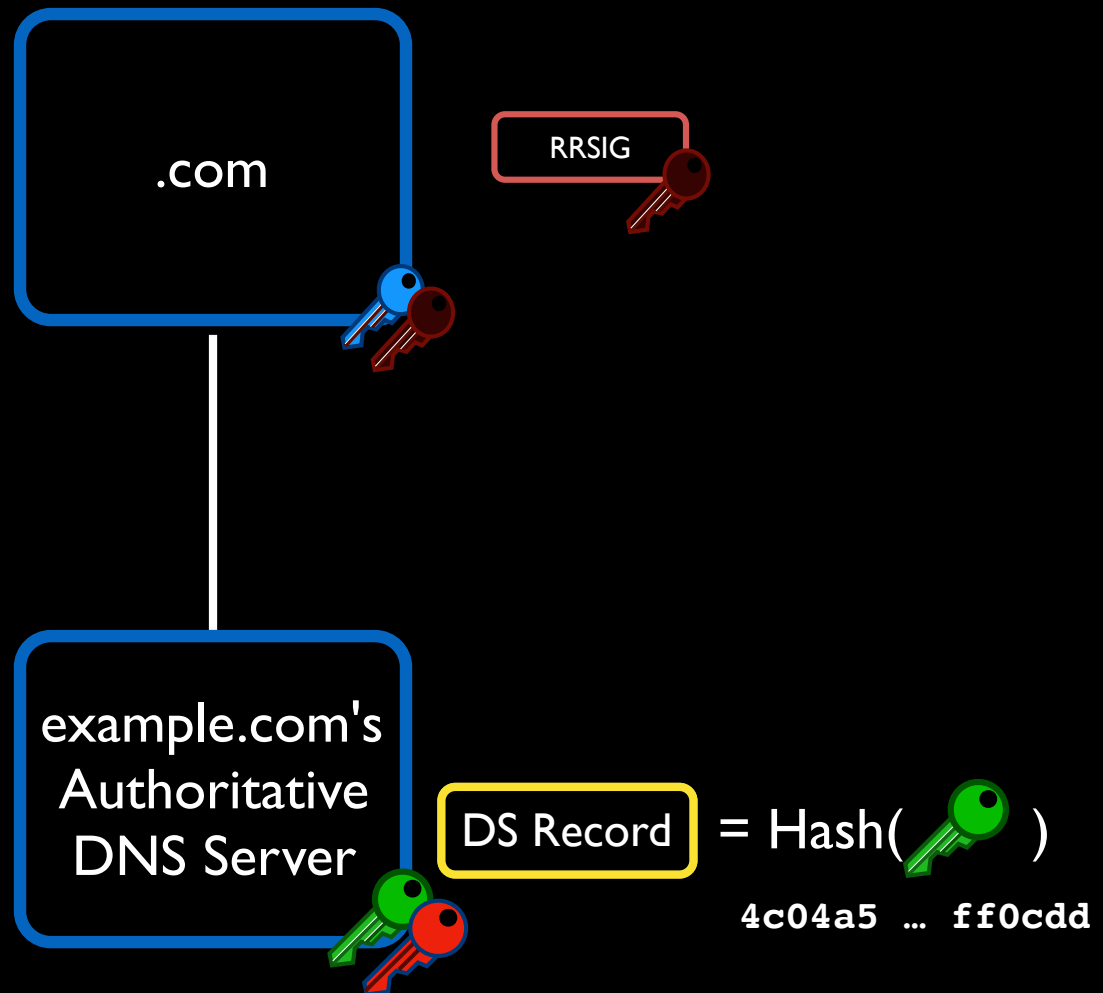
DNSKEY

DNSSEC 101

DNSSEC 101: Hierarchy Builds Trust

DNSSEC 101: Hierarchy Builds Trust
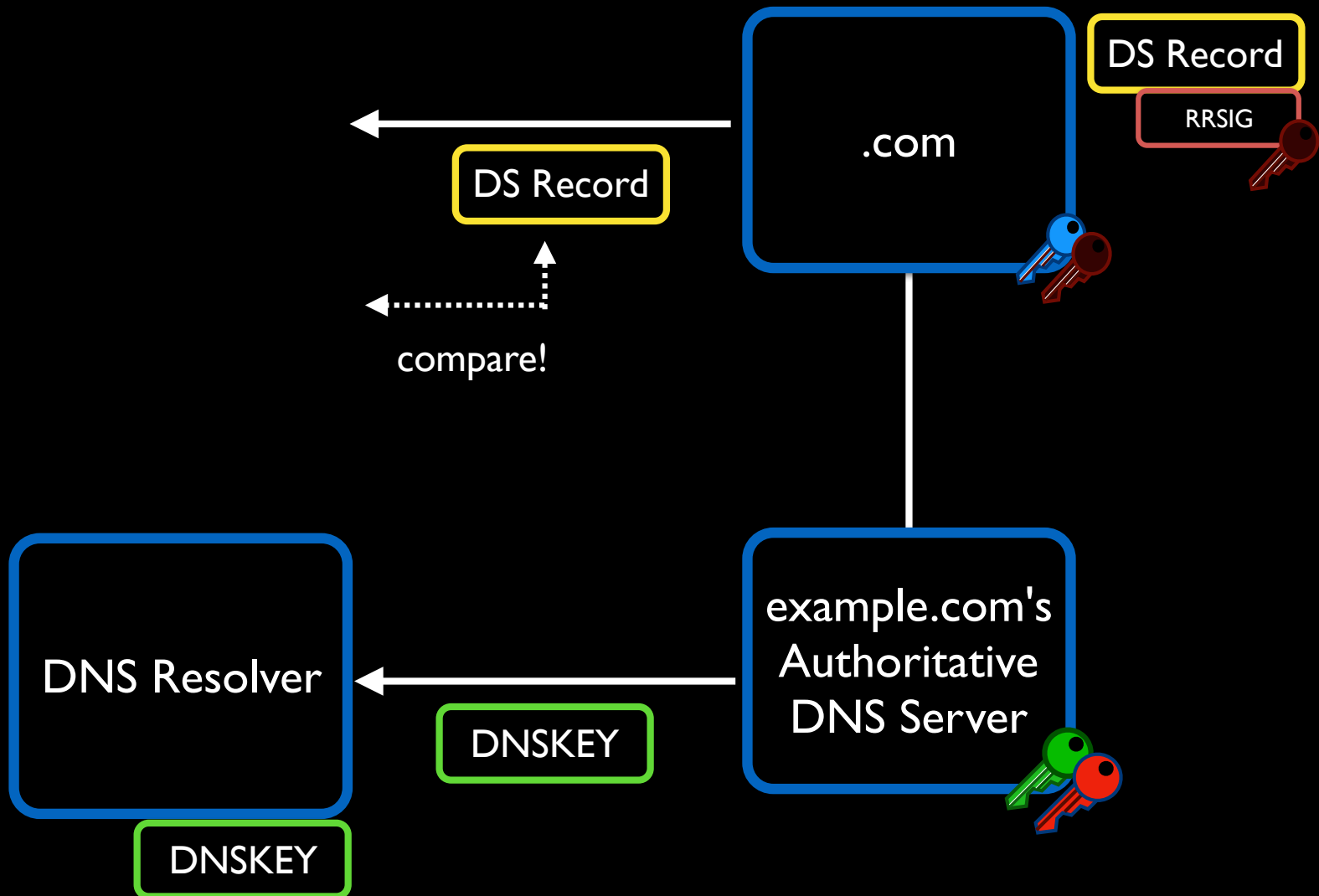
How to Deploy DNSSEC (Correctly)

DNSKEY → (1) Have DNSKEYs

RRSIGs → (2) Generate Signatures

DS record Uploads → (3) Generate and upload DS record to the parent zone
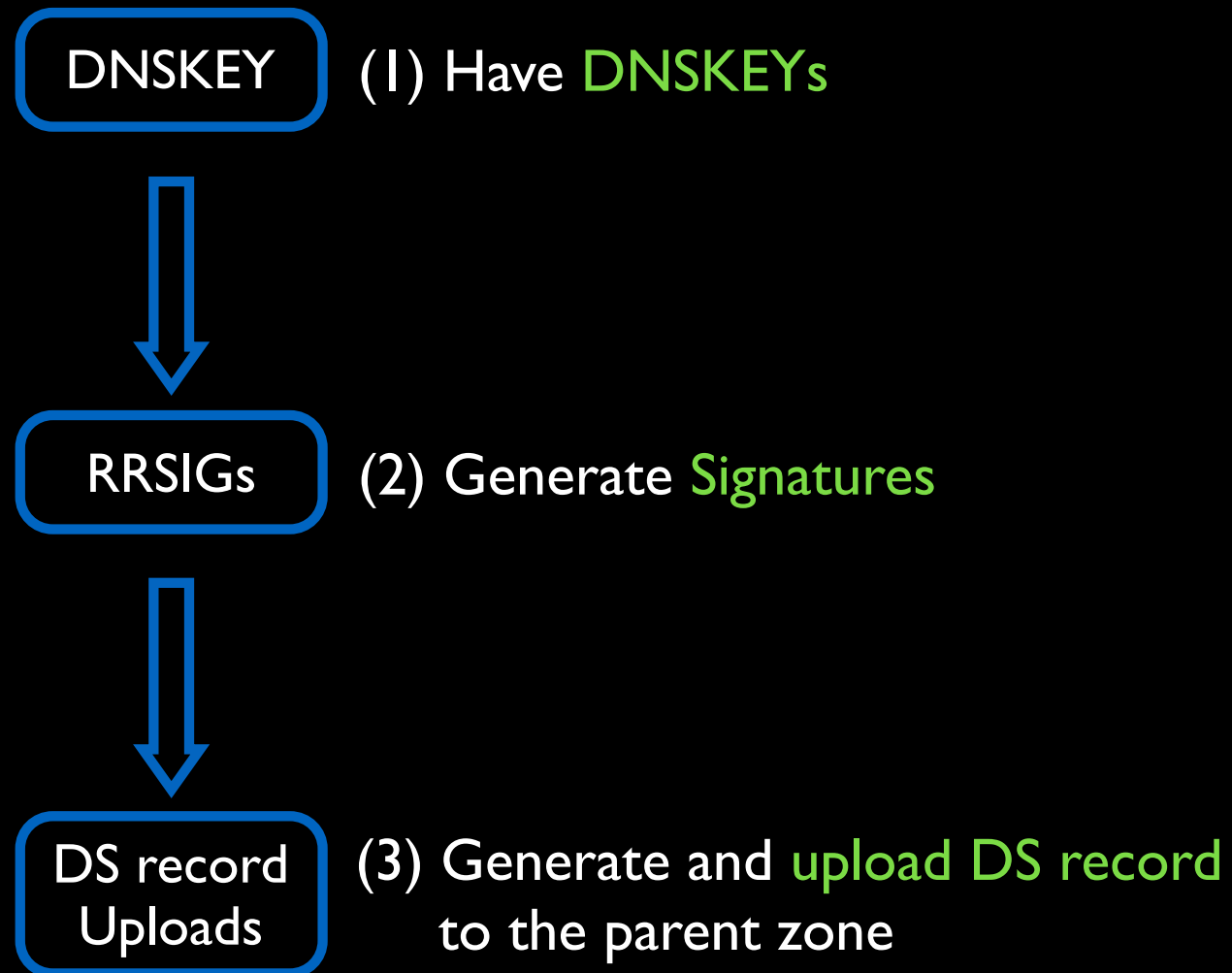
Scanning All Domains

	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

Deployment   DNSSEC deployment is rare, but growing

Generating Signatures

DNSKEY ~1.0%

RRSIGs ~0.3%

DS record
Uploads

Missing RRSIGs

RRSIGs are rarely missing (0.3%)
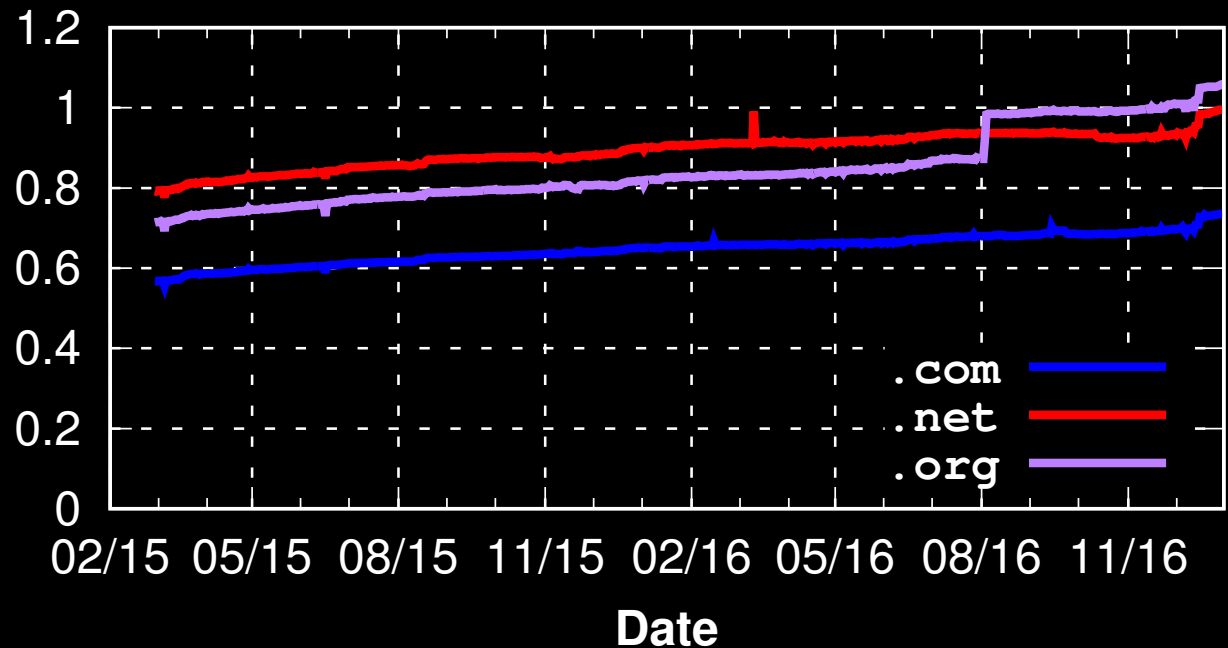
Building a Chain of Trust

DNSKEY — ~1.0%

RRSIGs — ~0.3%

DS record Uploads — ~30%

Percent of domains missing DS record

.com
.net
.org

02/15 05/15 08/15 11/15 02/16 05/16 08/16 11/16
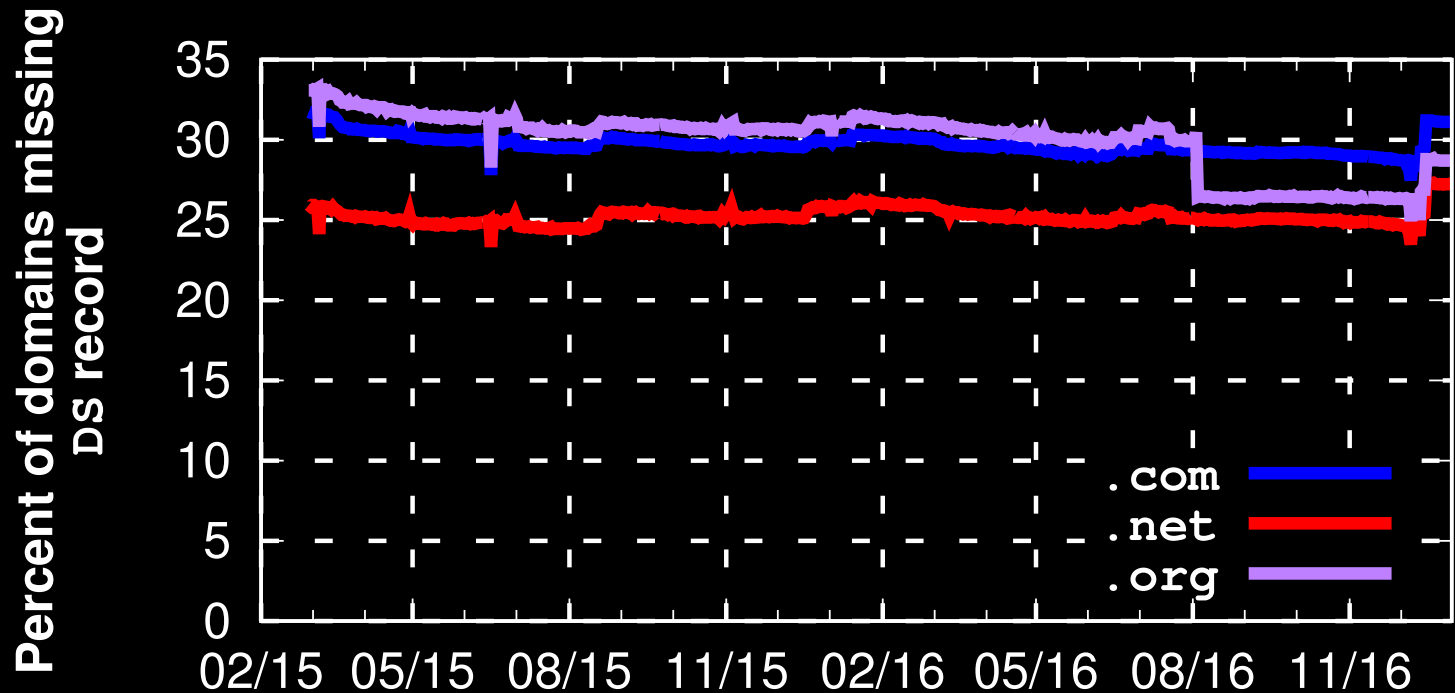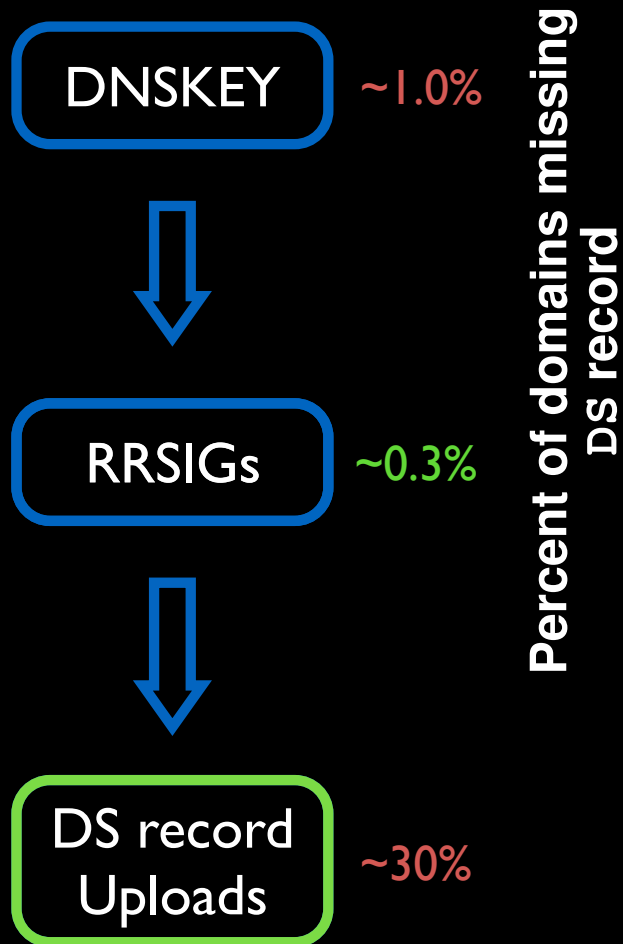
DS Records

Nearly 30% of domains DO NOT upload DS records!

Why does DNSSEC deployment remain so small?
Why are 30% of domains w/o DS records?

* A Longitudinal, End-to-End View of the DNSSEC Ecosystem [USENIX Security'17]

Open Question
(main part of this talk)

Why is so hard to deploy DNSSEC?

How does registrar policy impact the deployment?

Open Question
(main part of this talk)

Why is so hard to deploy DNSSEC?

How does registrar policy impact the deployment?

Deploying a DNSSEC on Your Server
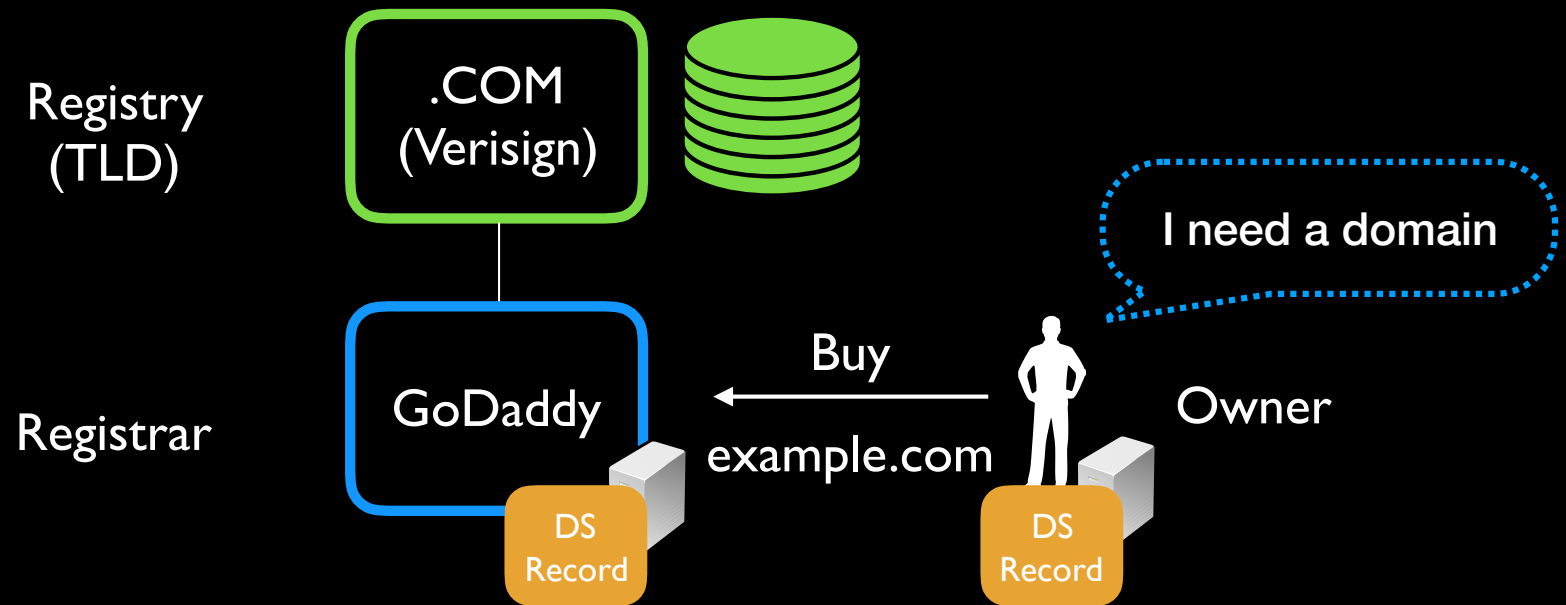
Third Party DNS Operator
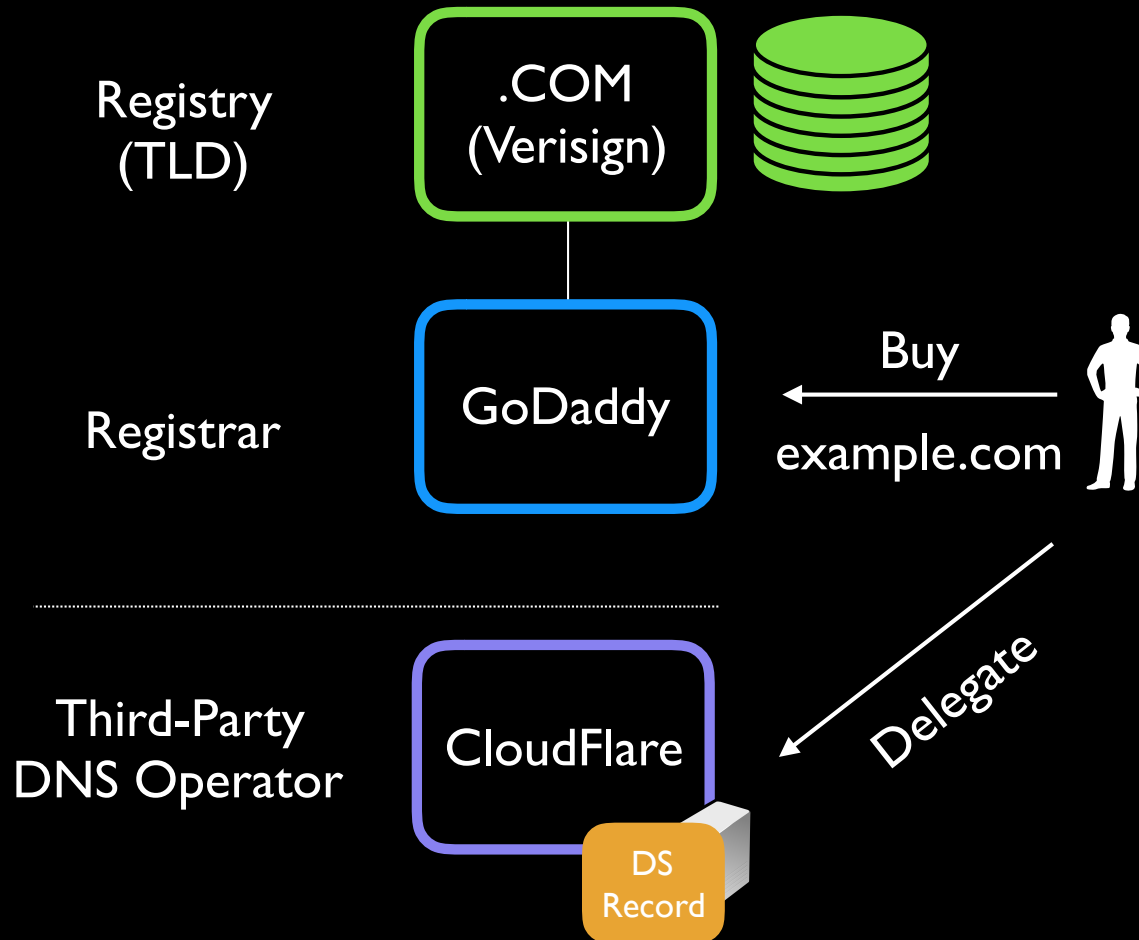
Registry (TLD)

.COM (Verisign)

Registrar

GoDaddy

Buy

example.com

Third-Party DNS Operator

CloudFlare

Delegate

DS Record

Third Party DNS Operator

Registry
(TLD)

.COM
(Verisign)

Registrar

GoDaddy

Buy

example.com

Third-Party
DNS Operator

CloudFlare

Delegate

Reseller

Registry (TLD) — .COM (Verisign)

Registrar — ASCIO

Reseller — Antagonist

Buy example.com

Delegate

Third-Party DNS Operator — CloudFlare

DS Record

18
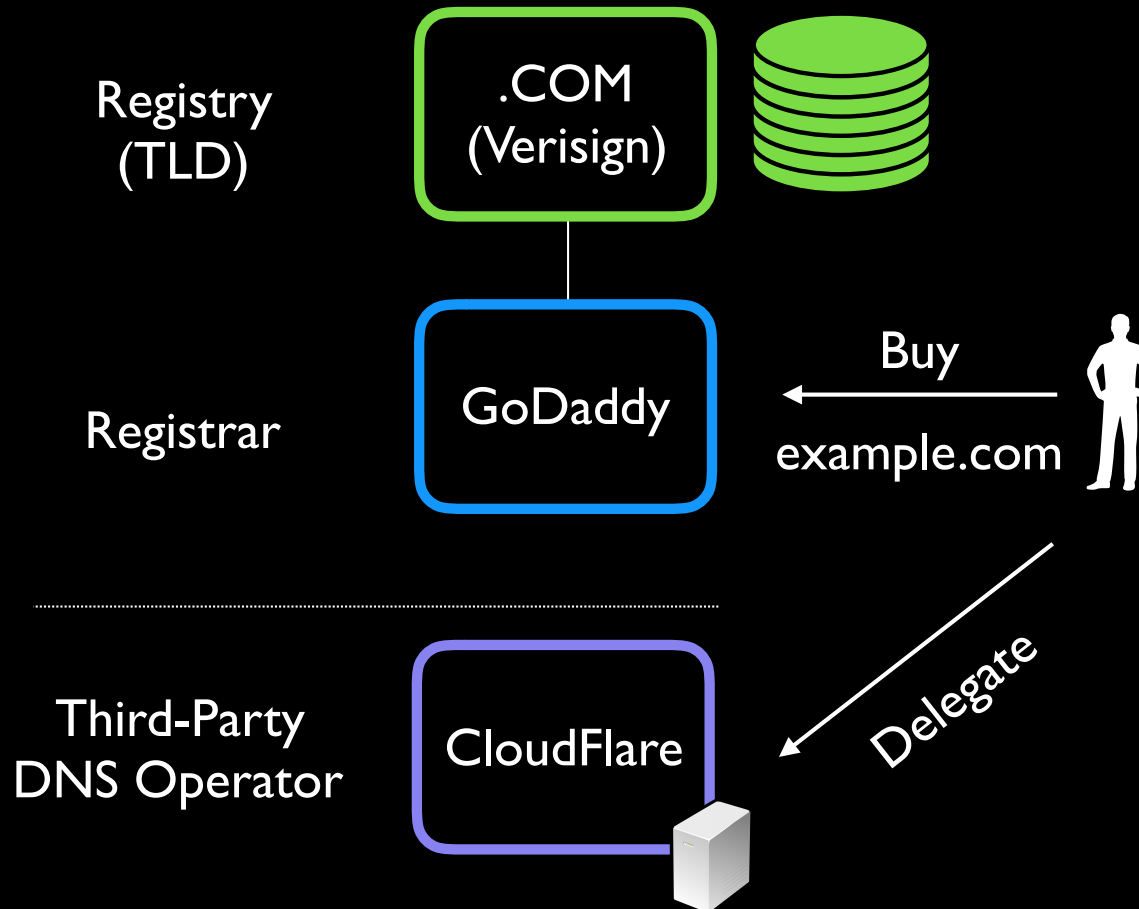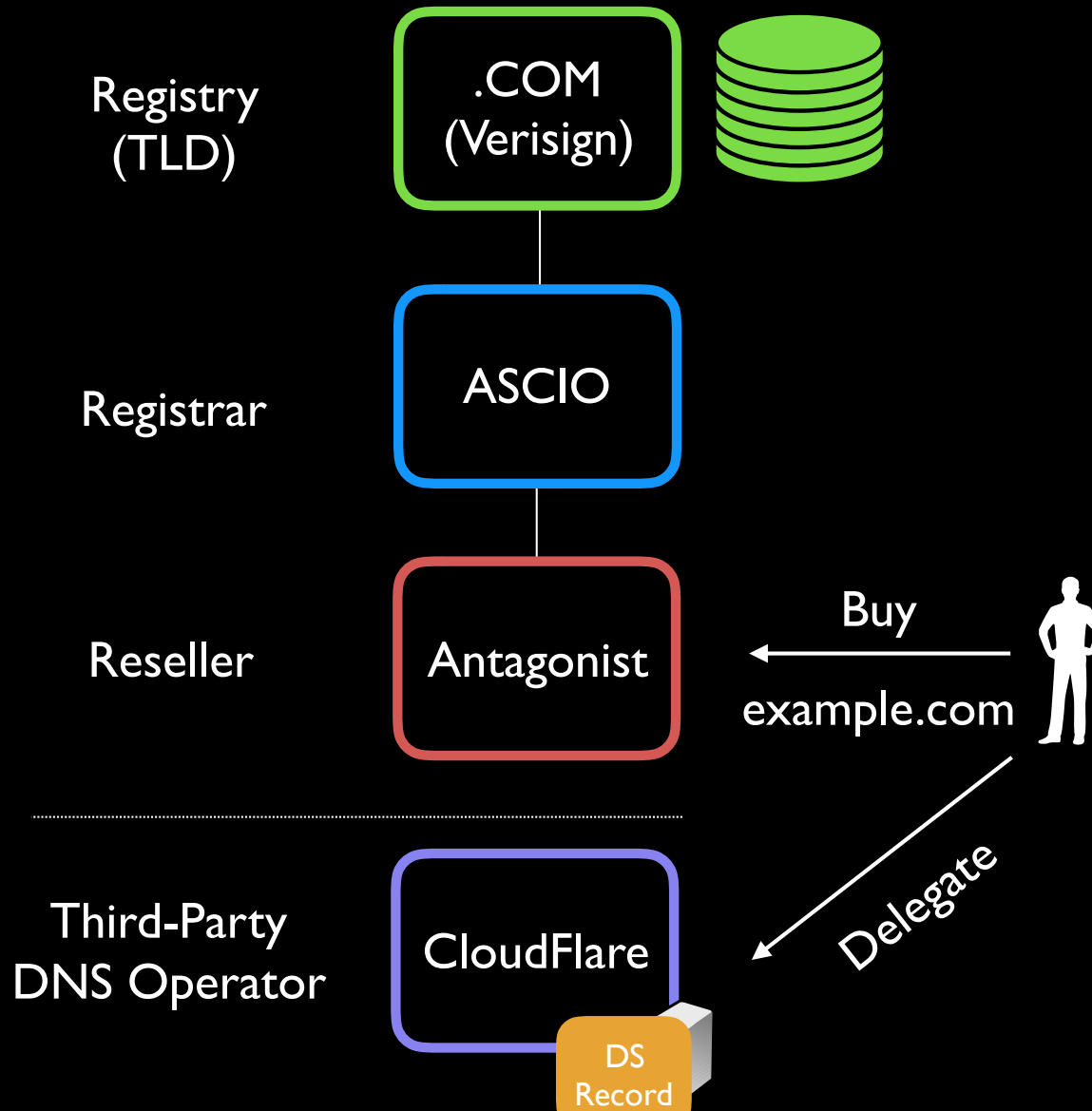
Open Question
(main part of this talk)

Why is so hard to deploy DNSSEC?
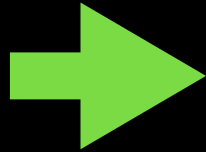
➡️ Popular registrar with lots of domains

Checking Registrar's DNSSEC Policy

Registrar
DNS Operator

Owner
DNS Operator

Registrar
Supports
DNSSEC?

↓

Registrar
Supports
DS upload?

↓

Registrar
Validates
DS record?
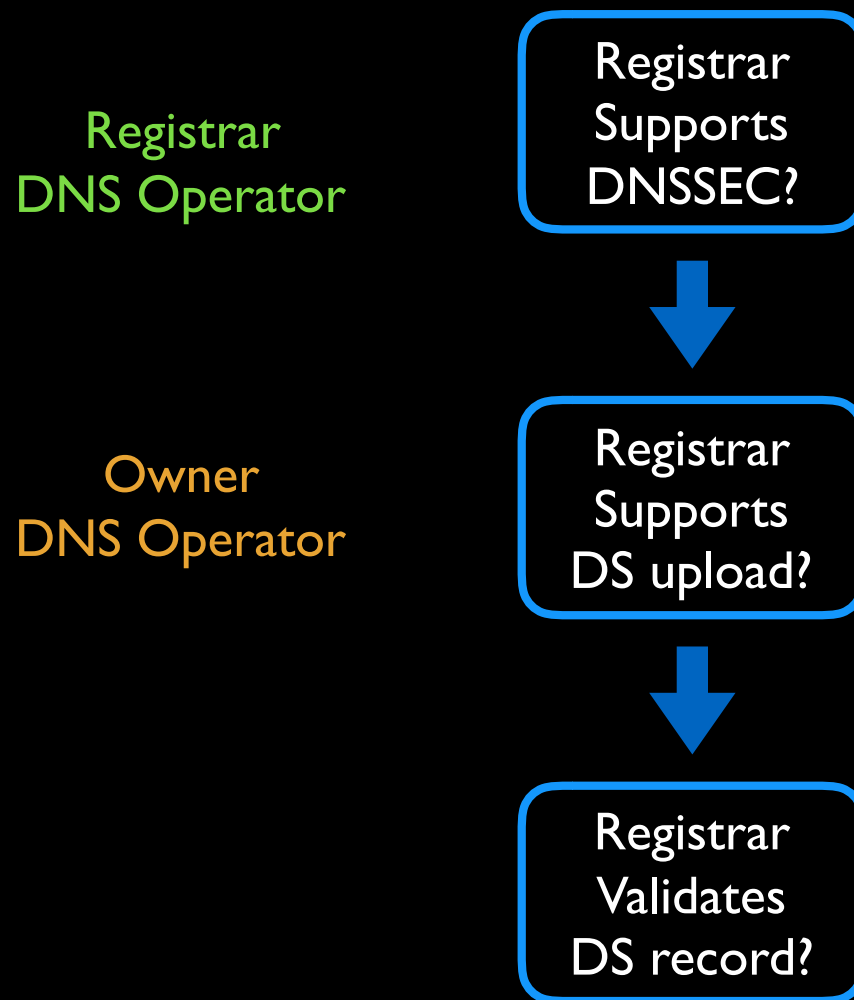
Anecdotal Examples

Experiment	Result
We saw the DNSKEY deployed (but not DS records) so asked why you don't upload DS records.	[1] They removed a DNSSEC menu [2] "*Most people do not understand DNS, so imagine the white faces when I mention DNSSEC*"
We asked a registrar to upload a DS record by email from the different email address than the one that registered	It was installed successfully
We asked a registrar to upload a DS record to our domain via web live chat	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*

4/20

Registrar Supports DNSSEC?

→

Registrar Supports DS upload?

→

Registrar Validates DS record?

Registrar	Registrar DNS Operator
GoDaddy (domaincontrol.com)	🟢
NameCheap (registrar-servers.com)	🟢
OVH (ovh.net)	🟢
Google (googledomains.com)	🟢
Alibaba (hichina.com)	❌
eNom (name-services.com)	❌
HostGator (hostgator.com)	❌
NameBright (namebrightdns.com)	❌
DreamHost (dreamhost.com)	❌
Amazon (aws-dns)	❌
123-reg (123-reg.co.uk)	❌
RightSide** (name.com)	❌
Network Solution (worldnic.com)	❌
Bluehost (bluehost.com)	❌
register.com (register.com)	❌
The others (5 registrars)	❌

* The results are as of July 2019
** Rightside was acquired by Donuts Inc, in July 2017

Popular Registrar's DNSSEC Policy

4/20

Registrar Supports DNSSEC?

↓

15/20

Registrar Supports DS upload?

↓

Registrar Validates DS record?

Registrar	Owner DNS Operator	
	DS Upload	
	Web	Email
GoDaddy (domaincontrol.com)	🟢	—
NameCheap (registrar-servers.com)	🟢	—
OVH (ovh.net)	🟢	—
Google (googledomains.com)	🟢	—
Alibaba (hichina.com)	🟢	—
eNom (name-services.com)	🟢	—
HostGator (hostgator.com)	🟢	—
NameBright (namebrightdns.com)	🟢	—
DreamHost (dreamhost.com)	🟢	—
Amazon (aws-dns)	🟢	—
123-reg (123-reg.co.uk)	🟢	—
RightSide* (name.com)	🟢	—
Network Solution (worldnic.com)	❌	🟢
Bluehost (bluehost.com)	❌	🟢
register.com (register.com)	❌	🟢
The others (5 registrars)	❌	❌

Popular Registrar's DNSSEC Policy

4/20

Registrar Supports DNSSEC?

15/20

Registrar Supports DS upload?

5/20

Registrar Validates DS record?

Registrar	Owner DNS Operator		DS Validation
	DS Upload		
	Web	Email	
GoDaddy (domaincontrol.com)	🟢	—	❌
NameCheap (registrar-servers.com)	🟢	—	❌
OVH (ovh.net)	🟢	—	🟢
Google (googledomains.com)	🟢	—	❌
Alibaba (hichina.com)	🟢	—	❌
eNom (name-services.com)	🟢	—	🟢
HostGator (hostgator.com)	🟢	—	🟢
NameBright (namebrightdns.com)	🟢	—	❌
DreamHost (dreamhost.com)	🟢	—	❌
Amazon (aws-dns)	🟢	—	⚠️
123-reg (123-reg.co.uk)	🟢	—	❌
RightSide* (name.com)	🟢	—	🟢
Network Solution (worldnic.com)	❌	🟢	❌
Bluehost (bluehost.com)	❌	🟢	❌
register.com (register.com)	❌	🟢	🟢
The others (5 registrars)	❌	❌	❌

Summary: Registrar's DNSSEC Support

	DNS Operator	# of Registrar	What this means to you
Support DNSSEC?	Registrar	4/20	If you don't want to run your own name server, most of the time, you CAN'T deploy DNSSEC (16/20)
	Owner	15/20	If you do want run your own nameserver, still you CAN'T deploy DNSSEC for 5/20
Check DS Validation	Owner	5/15	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

*DNSSEC and Its Potential for DDoS Attacks (IMC'14)

Case Study: Registrar's Policy

	Registrar DNS Operator		Owner DNS Operator	
	Support DNSSEC	Pricing	Support DNSSEC	Pricing
# of registrars	4	Free: 3	15	Free
		Paid: 1		

Registrars manage all DNS records

Registrars DO NOT need to manage DNS records at all

Comparison
2017 vs. 2019

July 2019 👏

Support DNSSEC?	DNS Operator	# of Registrar
Support DNSSEC?	Registrar	4/20
Support DNSSEC?	Owner	15/20
Check DS Validation	Owner	5/15

March 2017

of Registrar
3/20
11/20
2/11

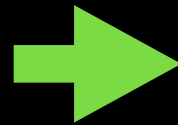**DNSSEC Deployment** Still a way to go, but it has been improved

Outline

Why is DNSSEC deployment so rare?

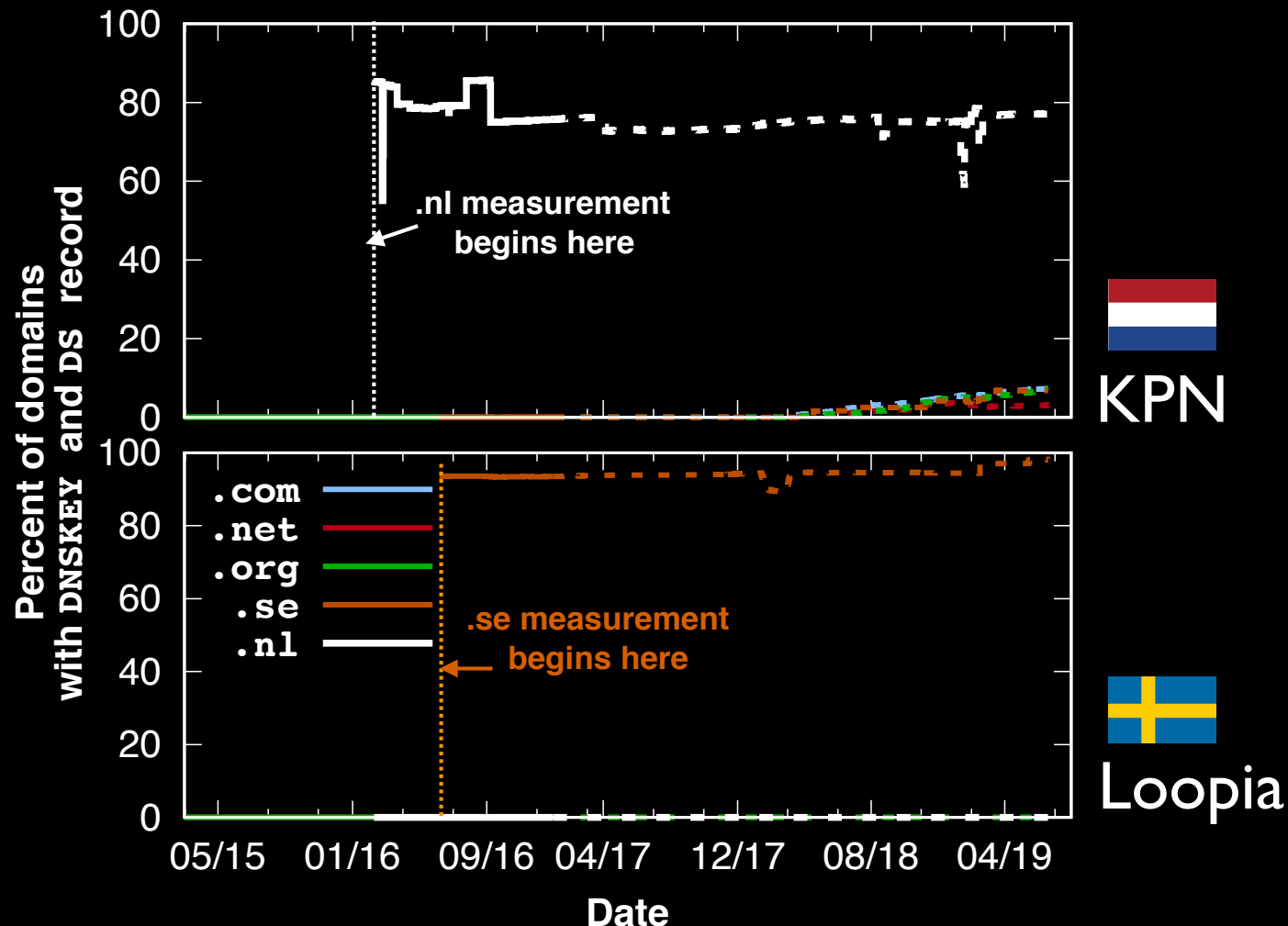How does a registrar policy impact the deployment?

We need historical dataset

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%

Scanning All Domains

TLD	Measurement Period (Daily Scan)	Domains	
		Total	Percent w/ DNSKEY
.com	2015/03/01 ~ 2019/06/19	140,438,505	
.net	2015/03/01 ~ 2019/06/19	13,408,301	
.org	2015/03/01 ~ 2019/06/19	10,066,388	
.nl	2016/02/09 ~ 2019/06/19	5,860,418	
.se	2016/06/07 ~ 2019/06/19	1,450,441	

[1] Registry: Financial Incentive

Percent of domains with DNSKEY and DS record (vertical axis, 0–100)

.nl measurement begins here

KPN

.com
.net
.org
.se
.nl

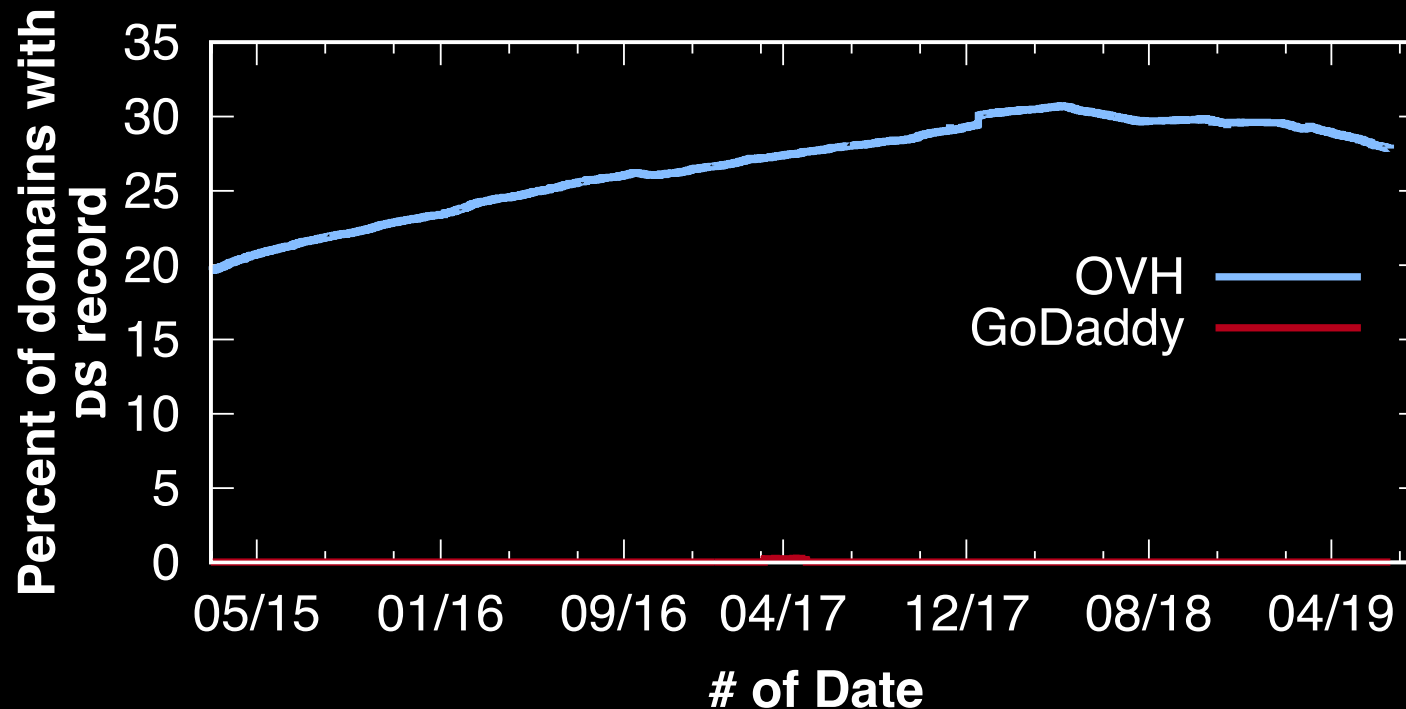.se measurement begins here

Loopia

Date: 05/15, 01/16, 09/16, 04/17, 12/17, 08/18, 04/19

Financial Incentive

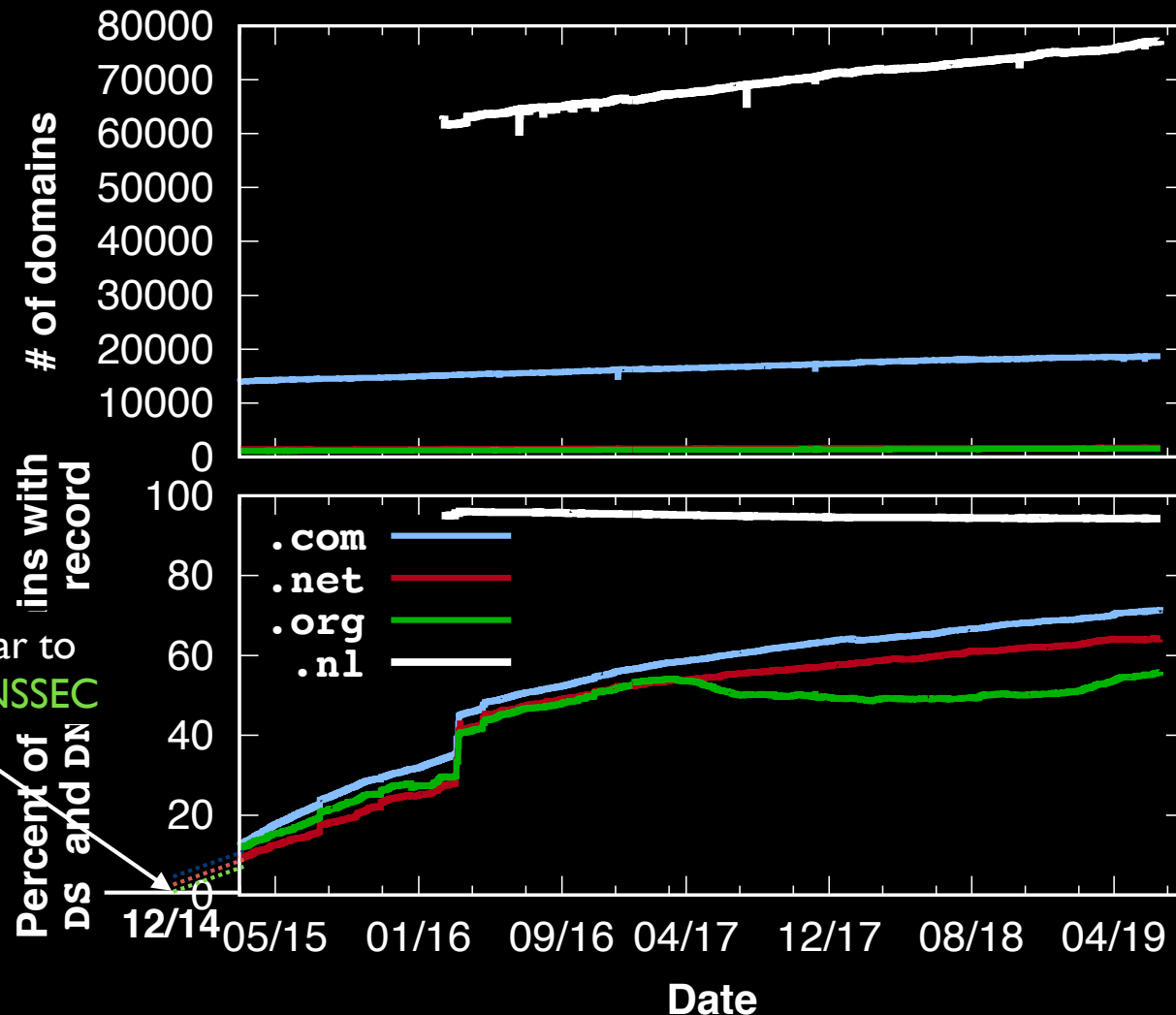Financial gain is a huge incentive for deploying DNSSEC

[2] Registrar: Free vs. Paid

Free vs. Paid

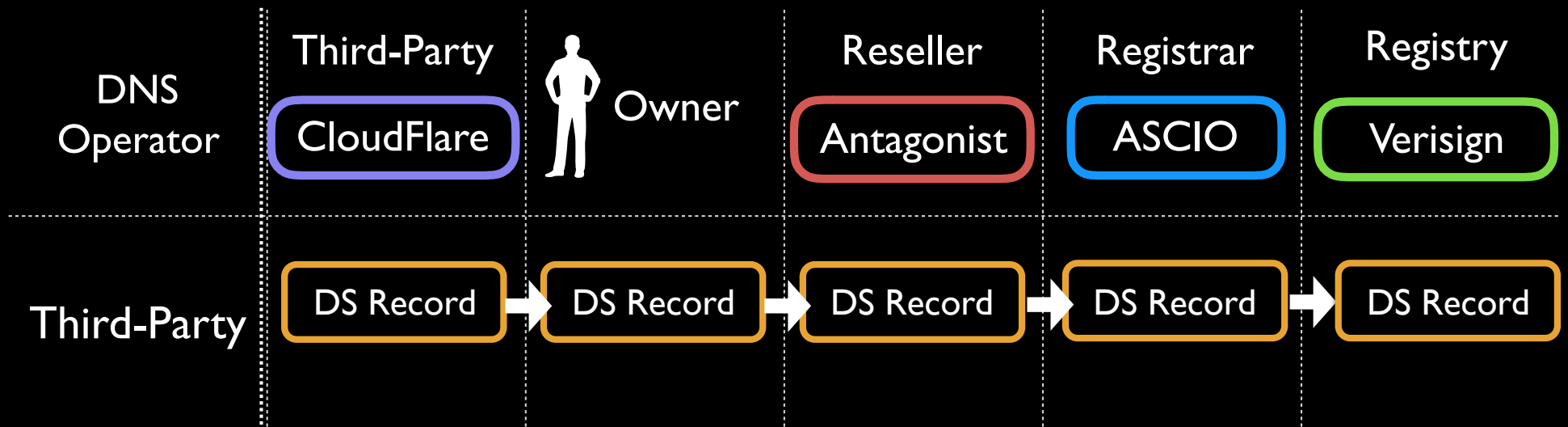Free DNSSEC support encourages users to deploy DNSSEC

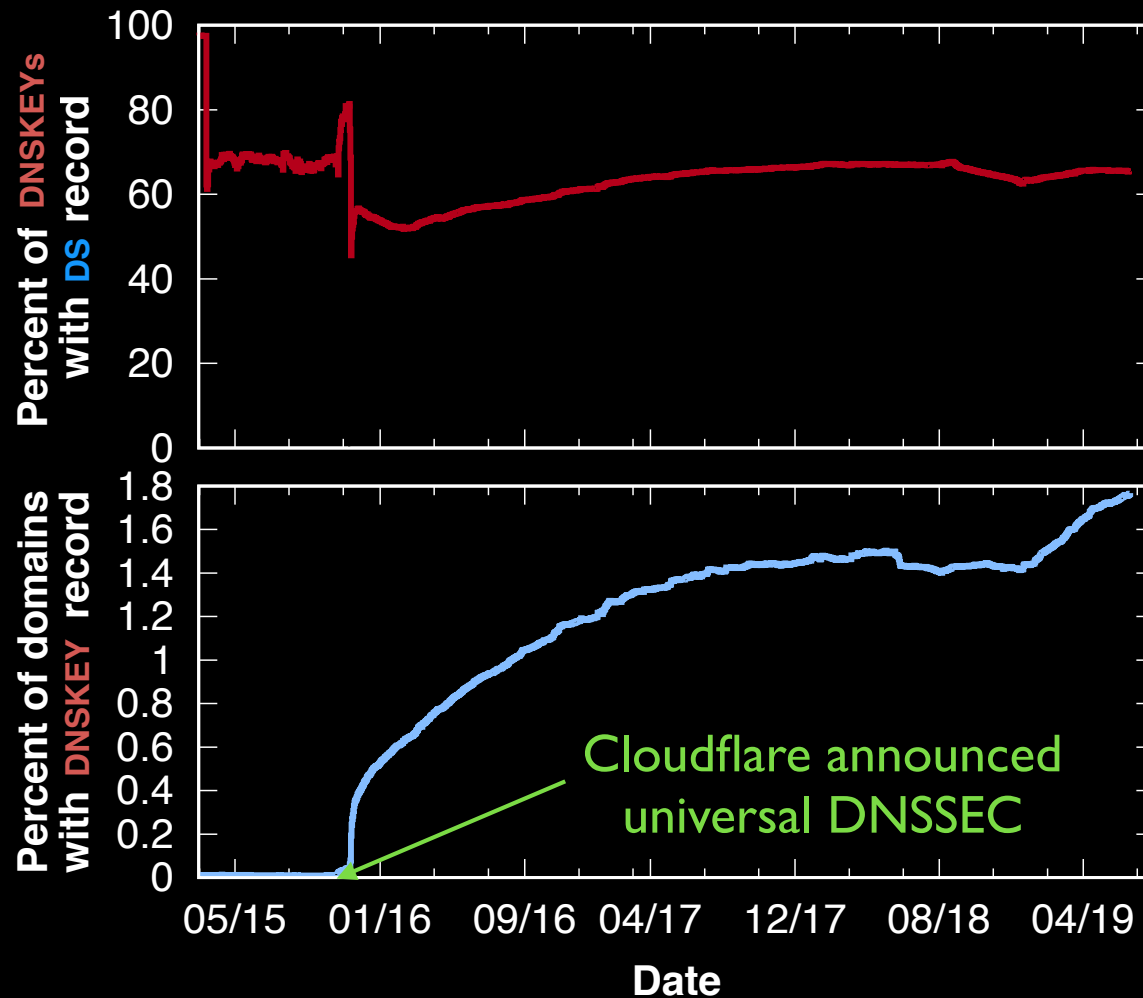# [3] Reseller (.com, .org, .net) vs. Registrar (.nl)

Changed their registrar to one that supports DNSSEC

Legend:
- .com
- .net
- .org
- .nl

Registrar vs. Reseller

Complex relationship between reseller and registrar also result in slow deployment of DNSSEC

[4] Third-Party DNS Operator <Cloudflare>

Cloudflare announced universal DNSSEC

Third-party DNS Operator

Deploying DNSSEC is even harder for users using third-party DNS Operators

Conclusion

- Registrars play a critical role in supporting DNSSEC today
  - Only 5 out of 20 registrars support DNSSEC on their authoritative nameservers
  - 15 out of 20 registrars support uploading a custom DS record
  - Comparing to 2017 it has been improved, but it requires more effort

- DNSSEC deployment depends on many policies
  - Registrar: Free
  - Registry: Financial incentive
  - Reseller: Beware to choose a partner (i.e., registrar)
  - Third-party: CDS/CDNSKEY