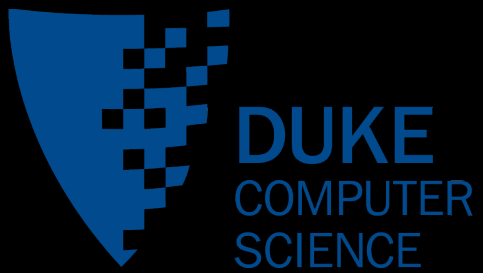
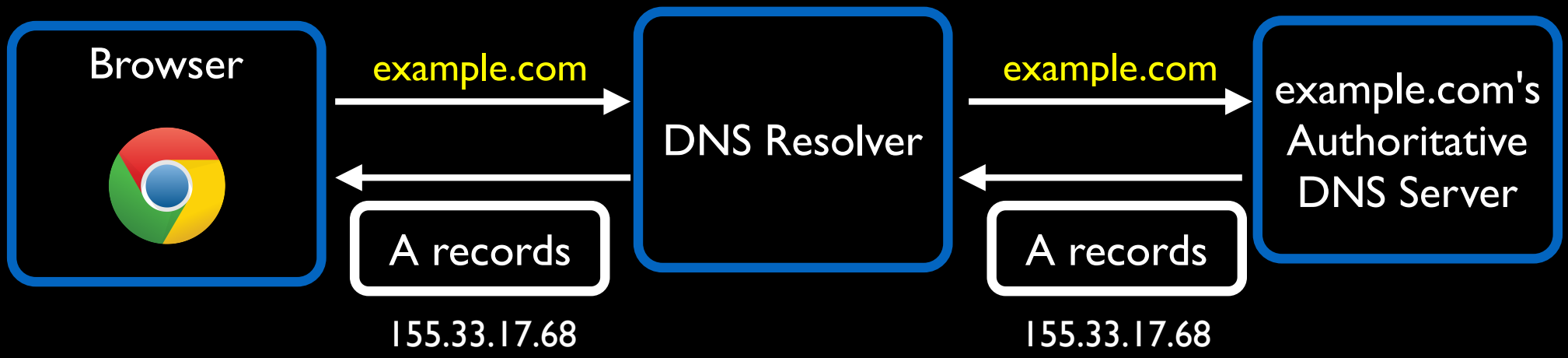
A Longitudinal, End-to-End View of the DNSSEC Ecosystem

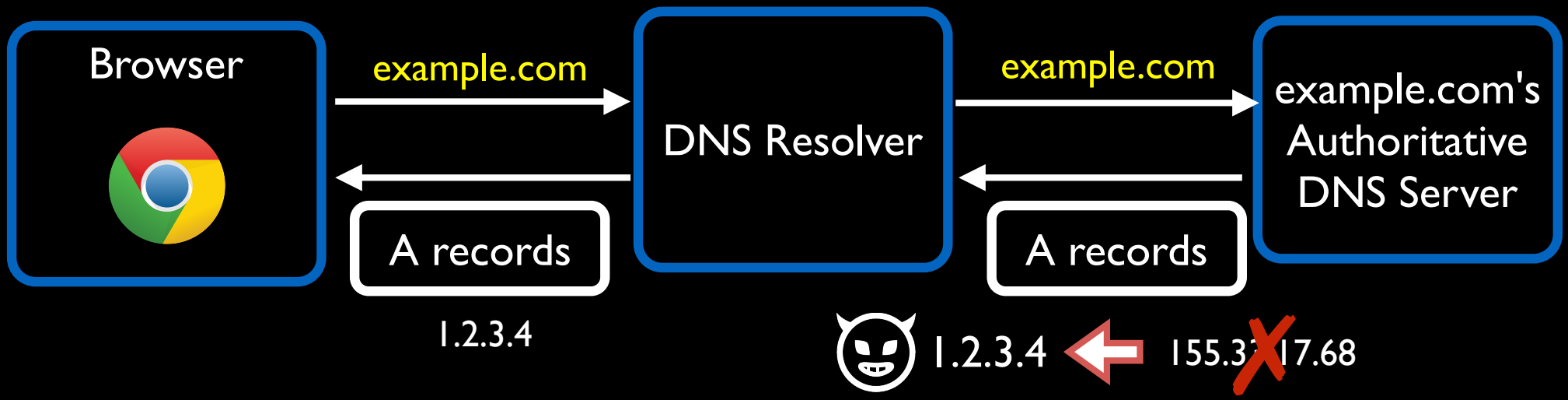
Taejoong (tijay) Chung, Roland van Rijswijk-Deij, Bala Chandrasekaran
David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, Christo Wilson



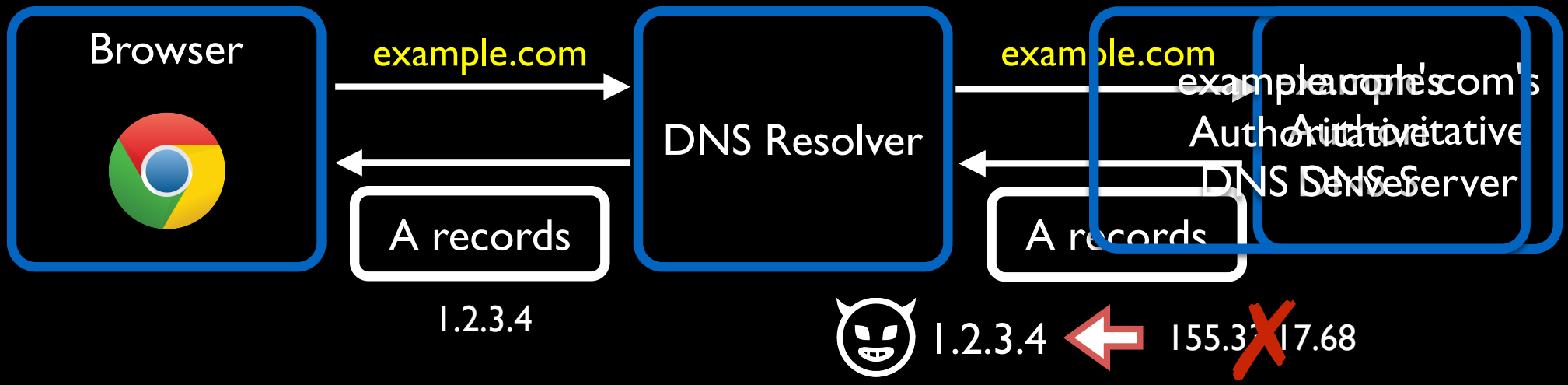
Domain Name System (DNS)



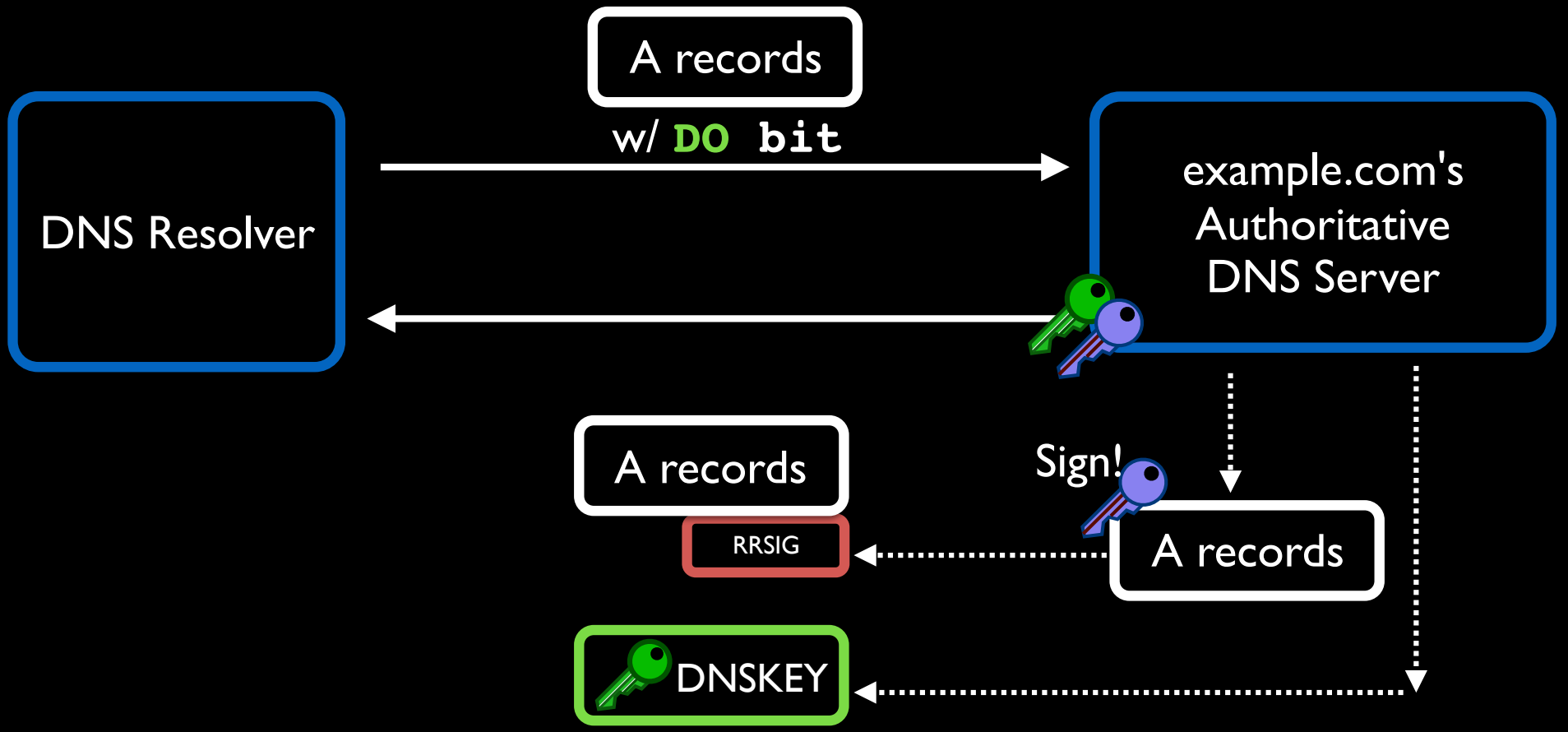
DNS Spoofing



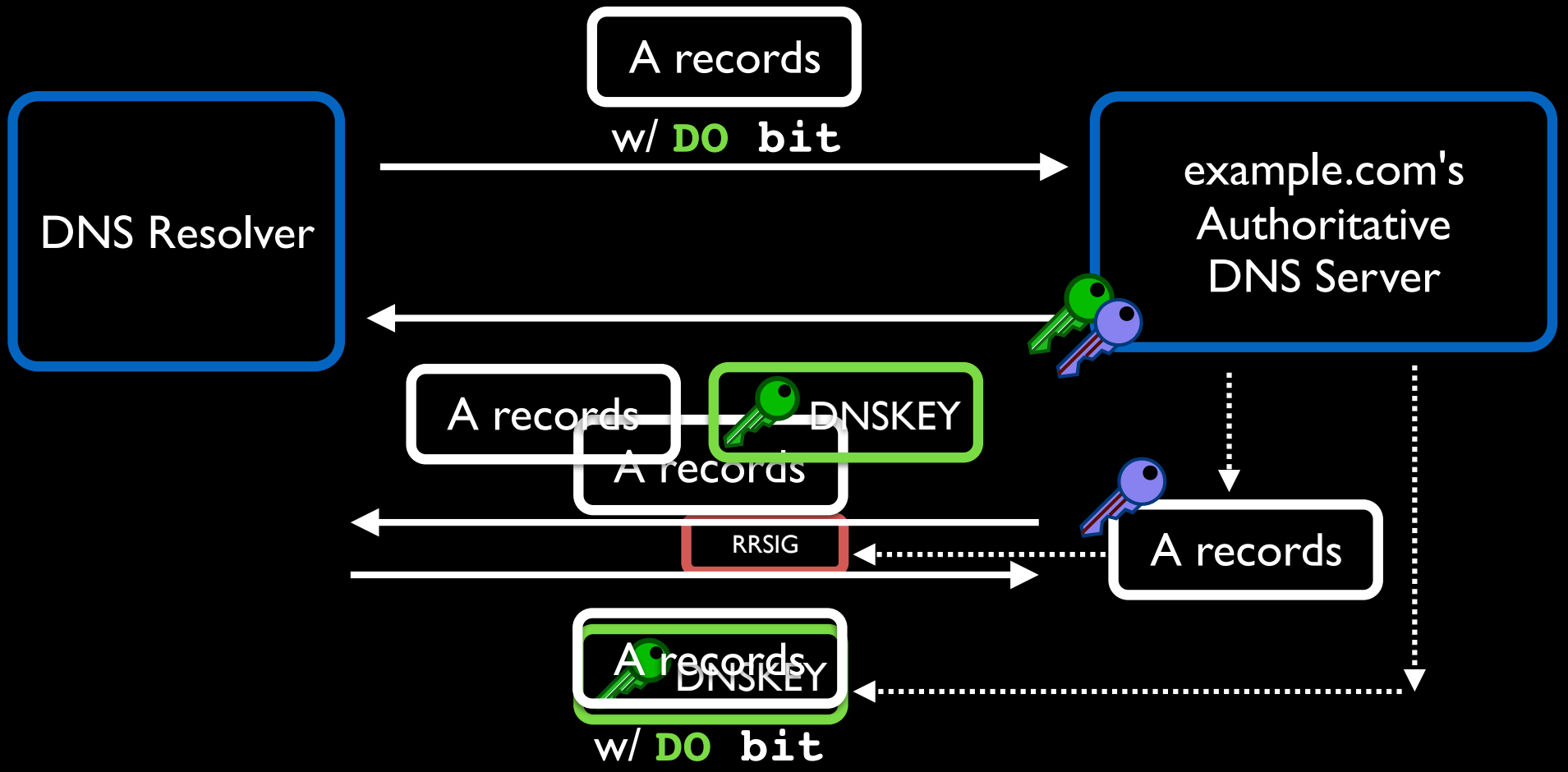
DNS Spoofing



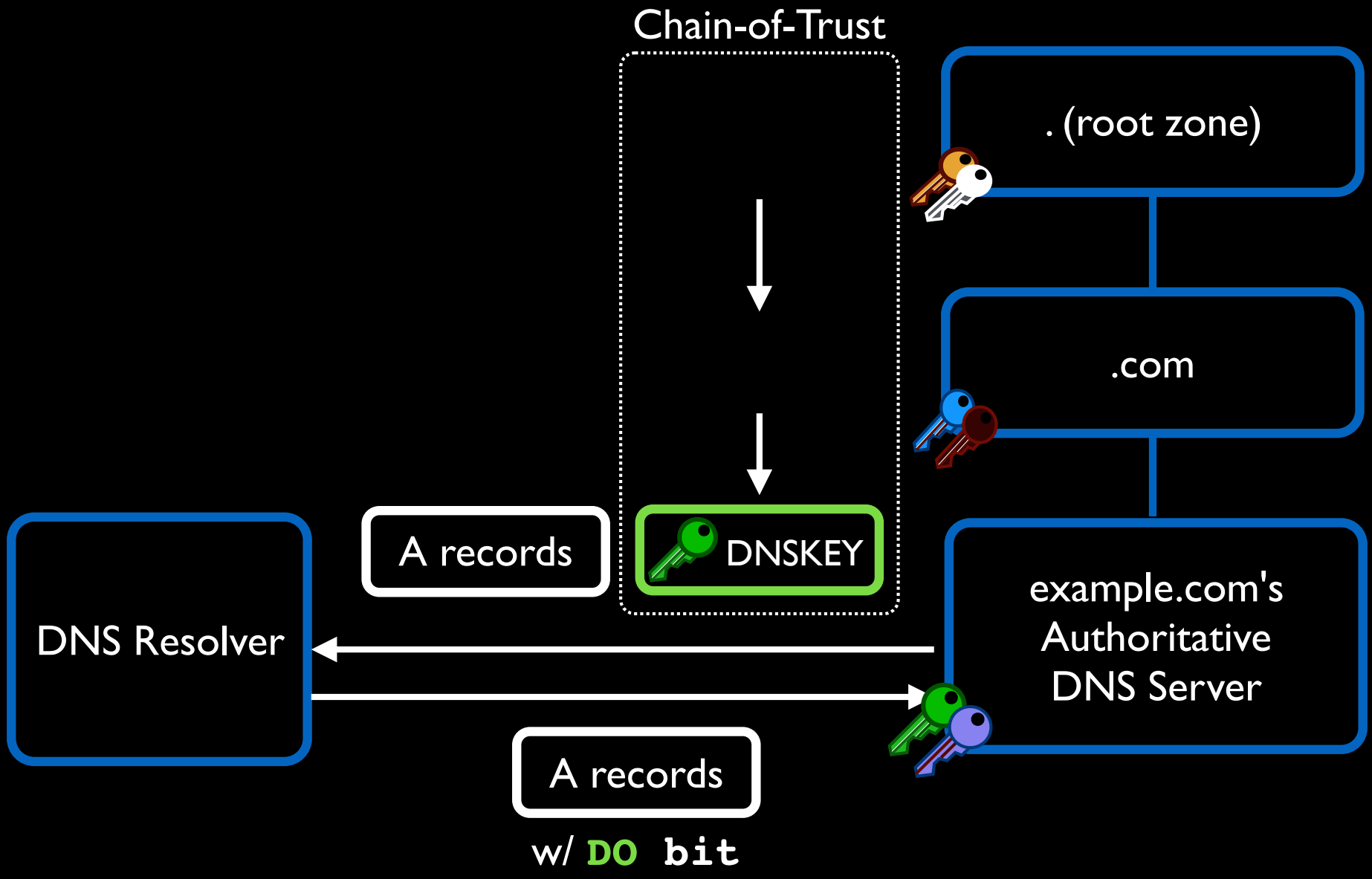
DNSSEC 101


A records
w/ DO bit
DNS Resolver
example.com's
Authoritative
DNS Server
A records
RRSIG
Sign!
A records
DNSKEY

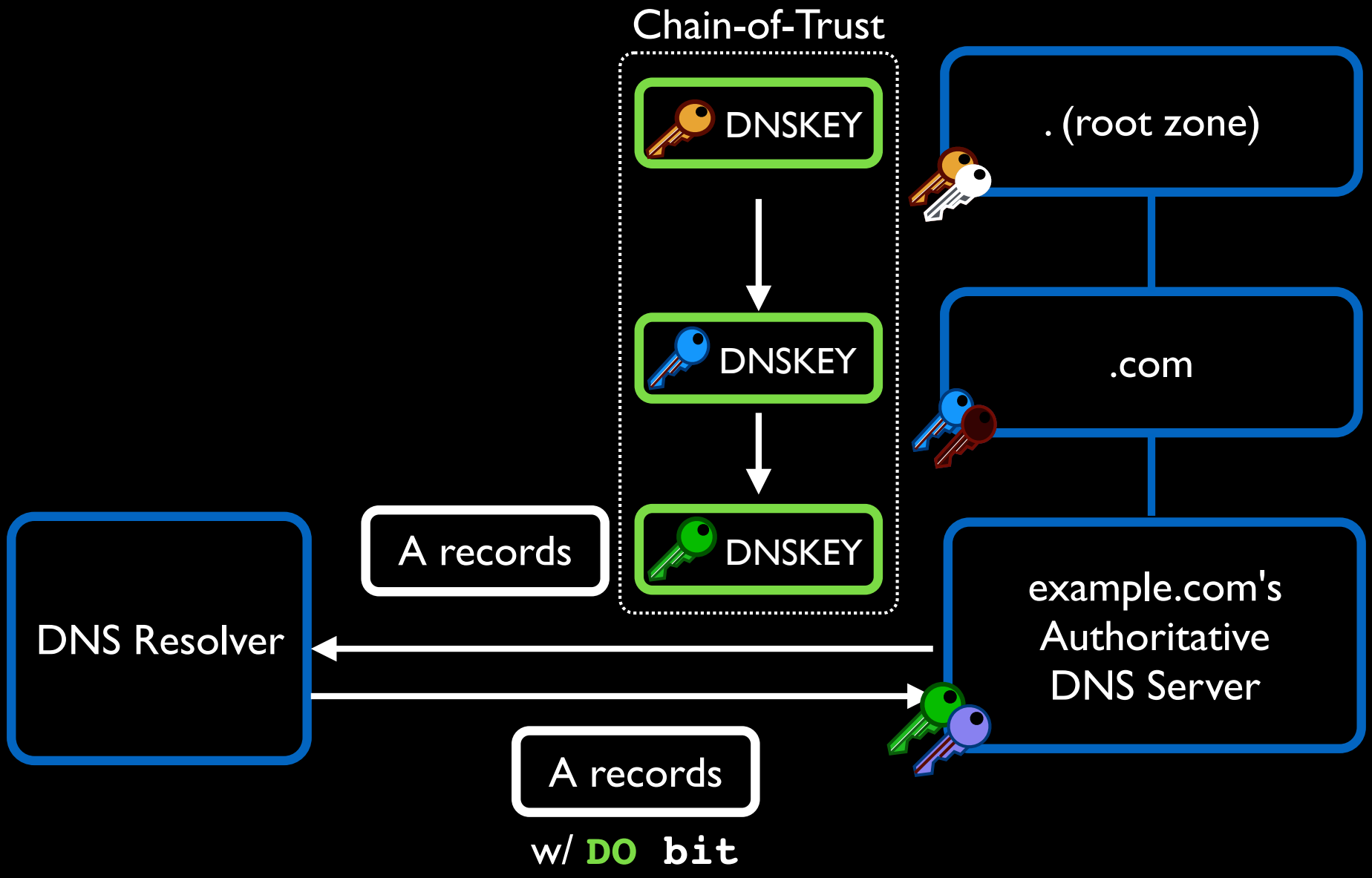
DNSSEC 101


A records
w/ DO bit
DNS Resolver
example.com's
Authoritative
DNS Server
A records
DNSKEY
A records
RRSIG
A records
A records
DNSKEY
w/ DO bit

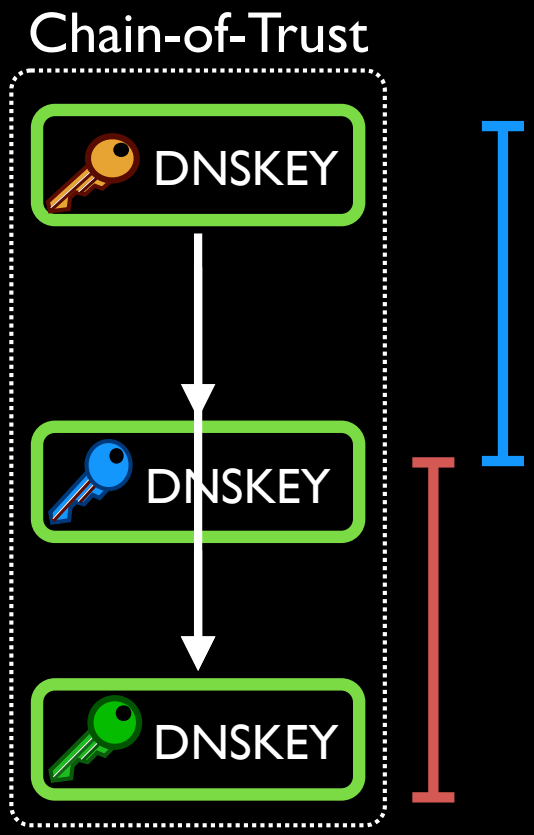
DNSSEC 101
Hierarchical Structure



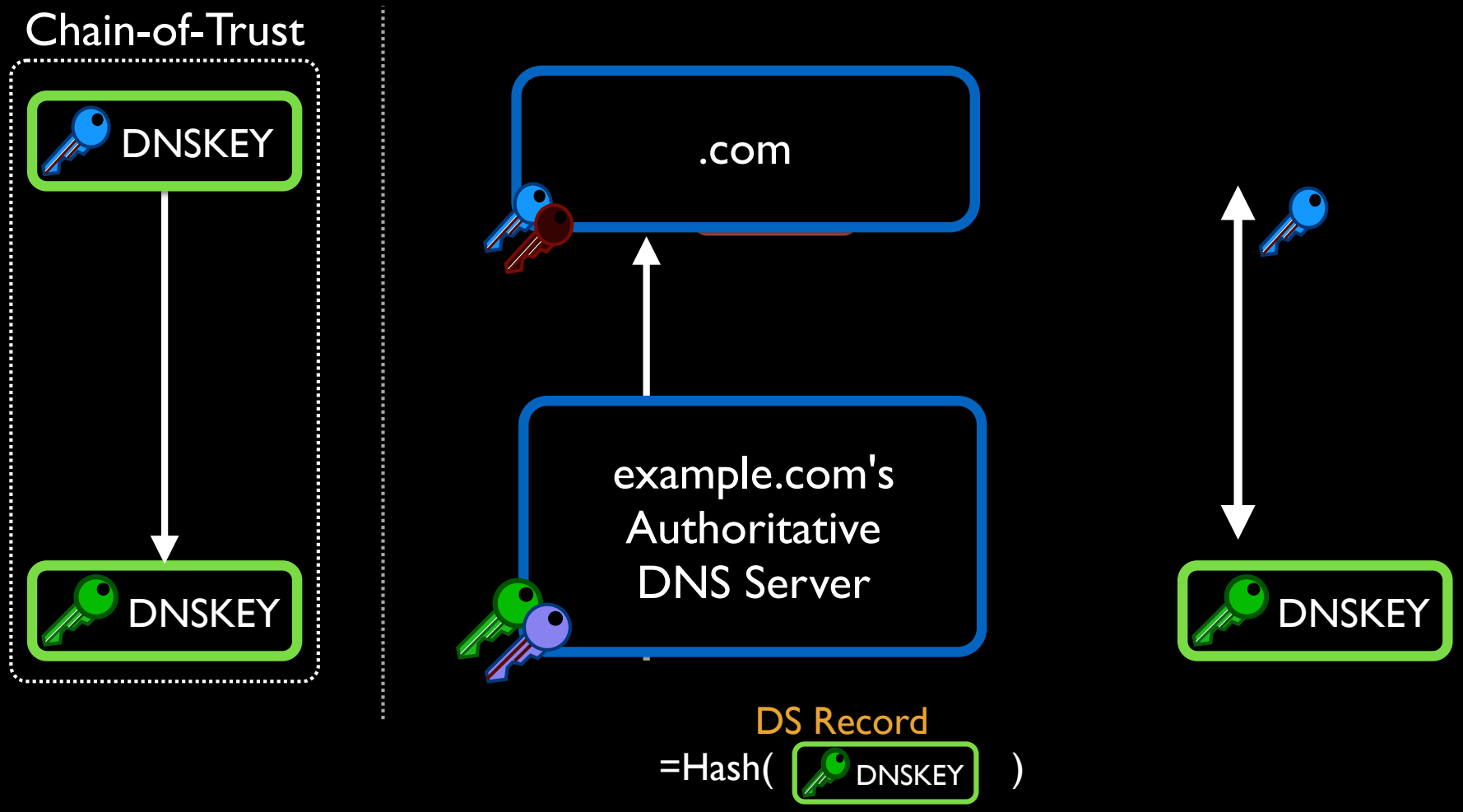
DNSSEC 101
Hierarchical Structure



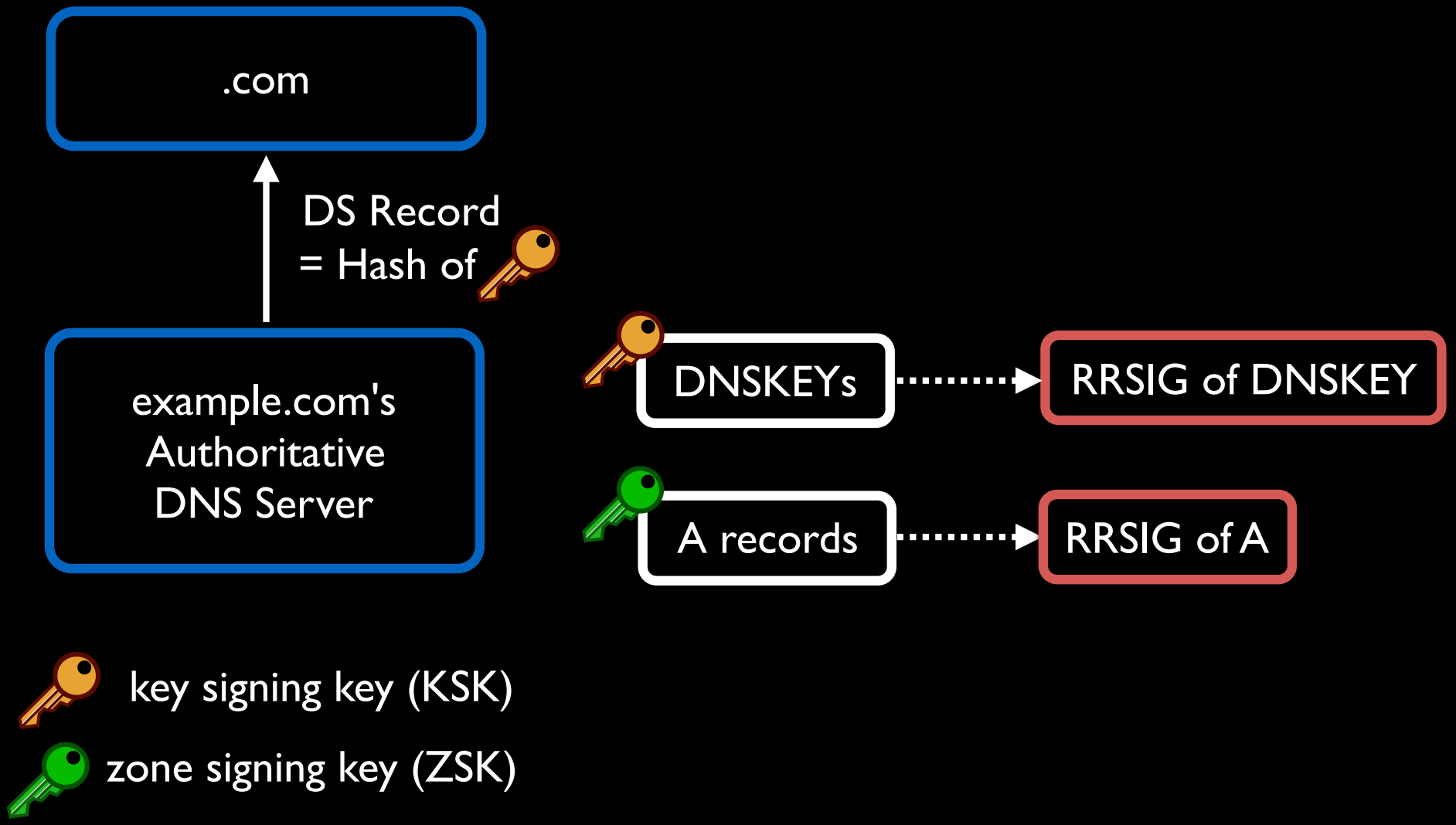
DNSSEC 101
Hierarchical Structure



DNSSEC 101
Hierarchical Structure



DNSSEC 101
Two DNSKEYs



Summary of DNSSEC 101

- Three essential elements for DNSSEC
  - RRSIG
  - 

  - DS Record
    - has to be uploaded to the parent zone
- Resolvers need to verify all signatures along the chains of trust
- DNSSEC can only function correctly when all principals (server and resolver) work correctly

Open Question

How's the DNSSEC PKI ecosystem managed?

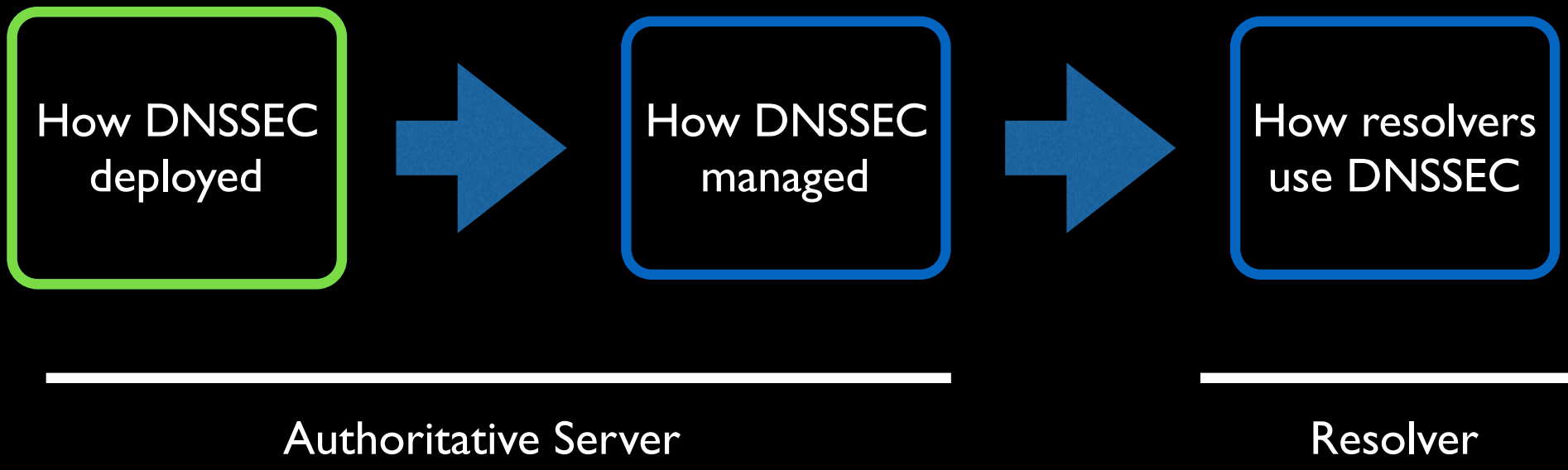
Contribution

Longitudinal

Comprehensive

All Angles

Outline


How DNSSEC deployed
How DNSSEC managed
How resolvers use DNSSEC
Authoritative Server
Resolver

Correct Deployment for Authoritative Servers

(1) Have DNSKEYs

(2) Generate Signatures

(3) Valid Signatures
(Not expired, correctly signed)

(4) Generate and upload DS record
to the parent zone

(5) Valid DS record
(matched with DNSKEYs)

Dataset

	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

* https://openintel.nl/

DNSSEC Deployment

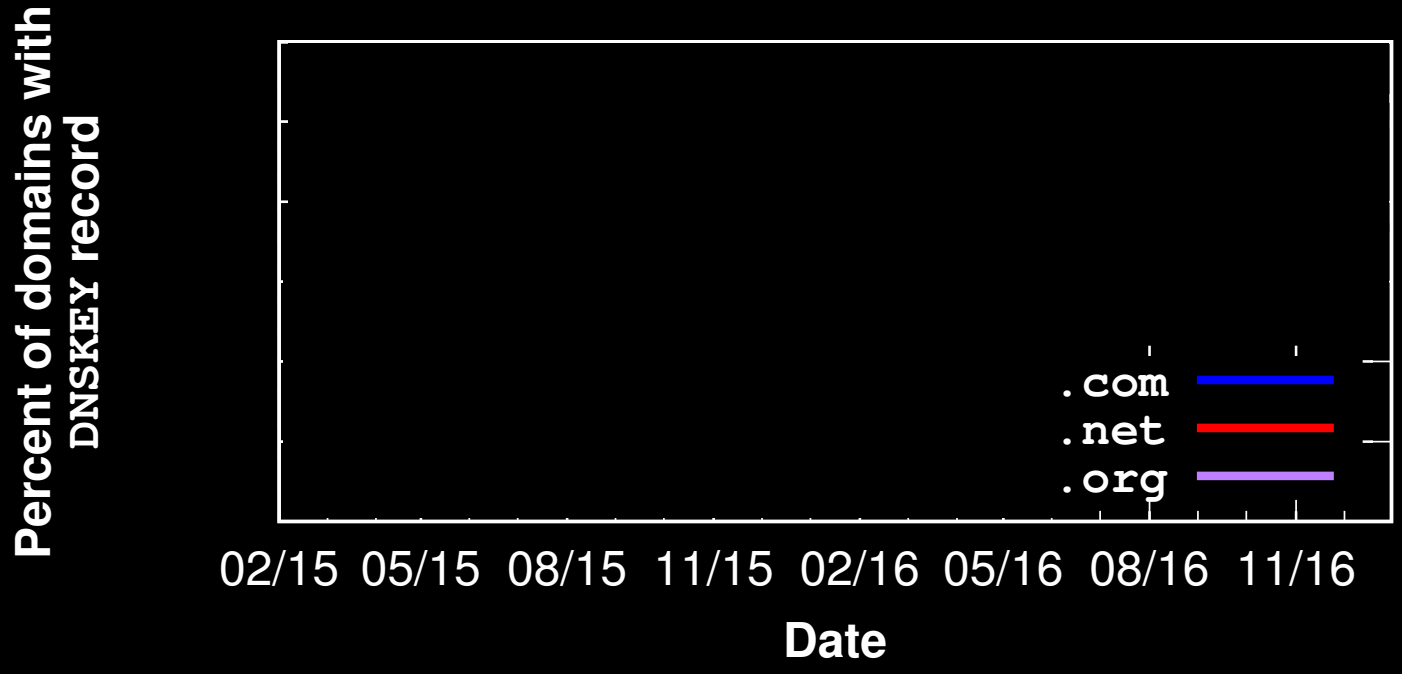
DNSKEY ~1.0%

RRSIGs

Valid RRSIGs

DS record Uploads

Valid DS record



Deployment

DNSSEC deployment is rare, but growing

Are they correctly deployed?

Missing RRSIG records

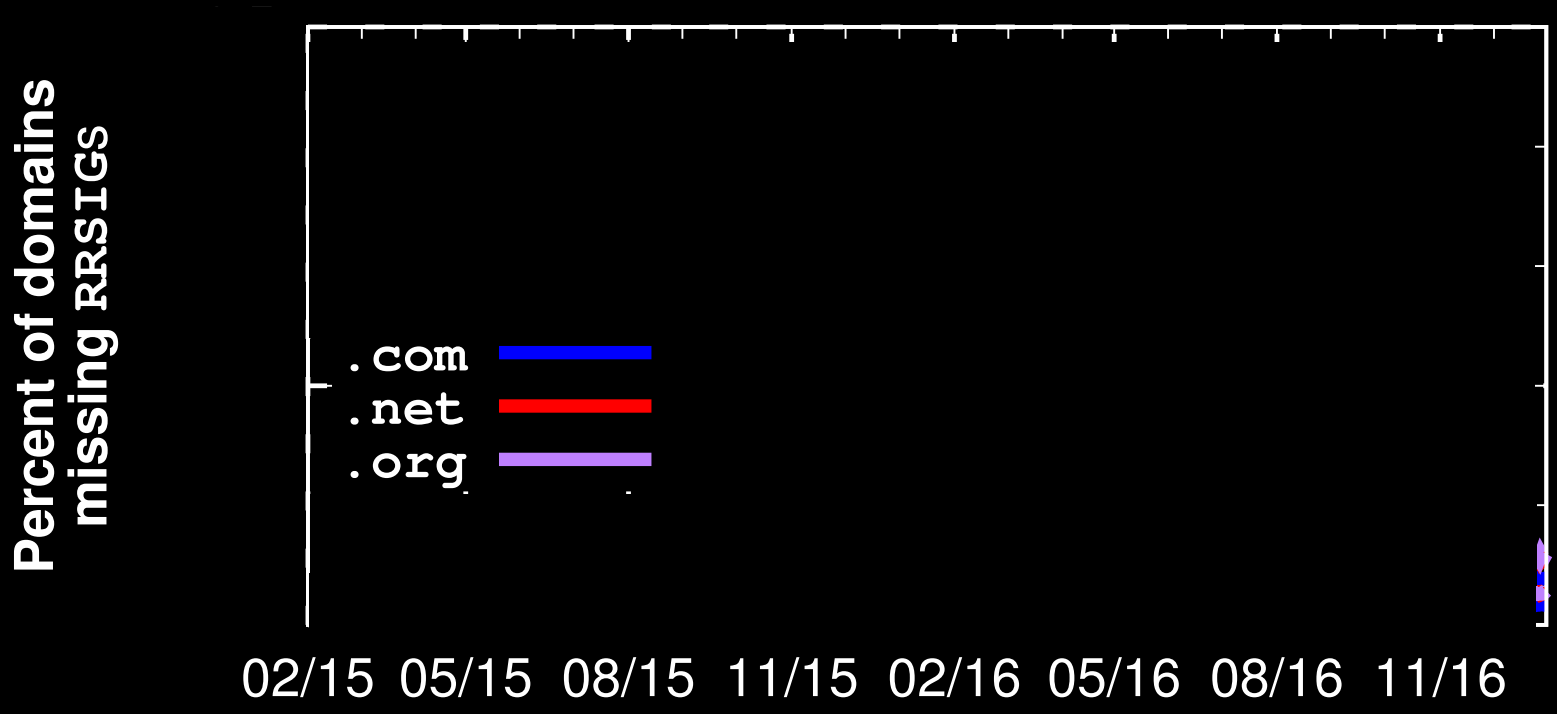
DNSKEY ~1.0%

RRSIGs ~0.3%

Valid RRSIGs

DS record Uploads

Valid DS record



Missing RRSIGs

RRSIGs are rarely missing (0.3%)

Incorrect RRSIG records

DNSKEY ~1.0%

RRSIGs ~0.3%

Valid RRSIGs ~0.5%

DS record Uploads

Valid DS record

Invalid RRSIGs

RRSIGs are managed well (~0.5%)

Missing DS records

DNSKEY ~1.0%

RRSIGs ~0.3%

Valid RRSIGs ~0.5%

DS record Uploads ~30%

Valid DS record

DS Records

Nearly 30% of domains DO NOT upload DS records!

Incorrect DS records

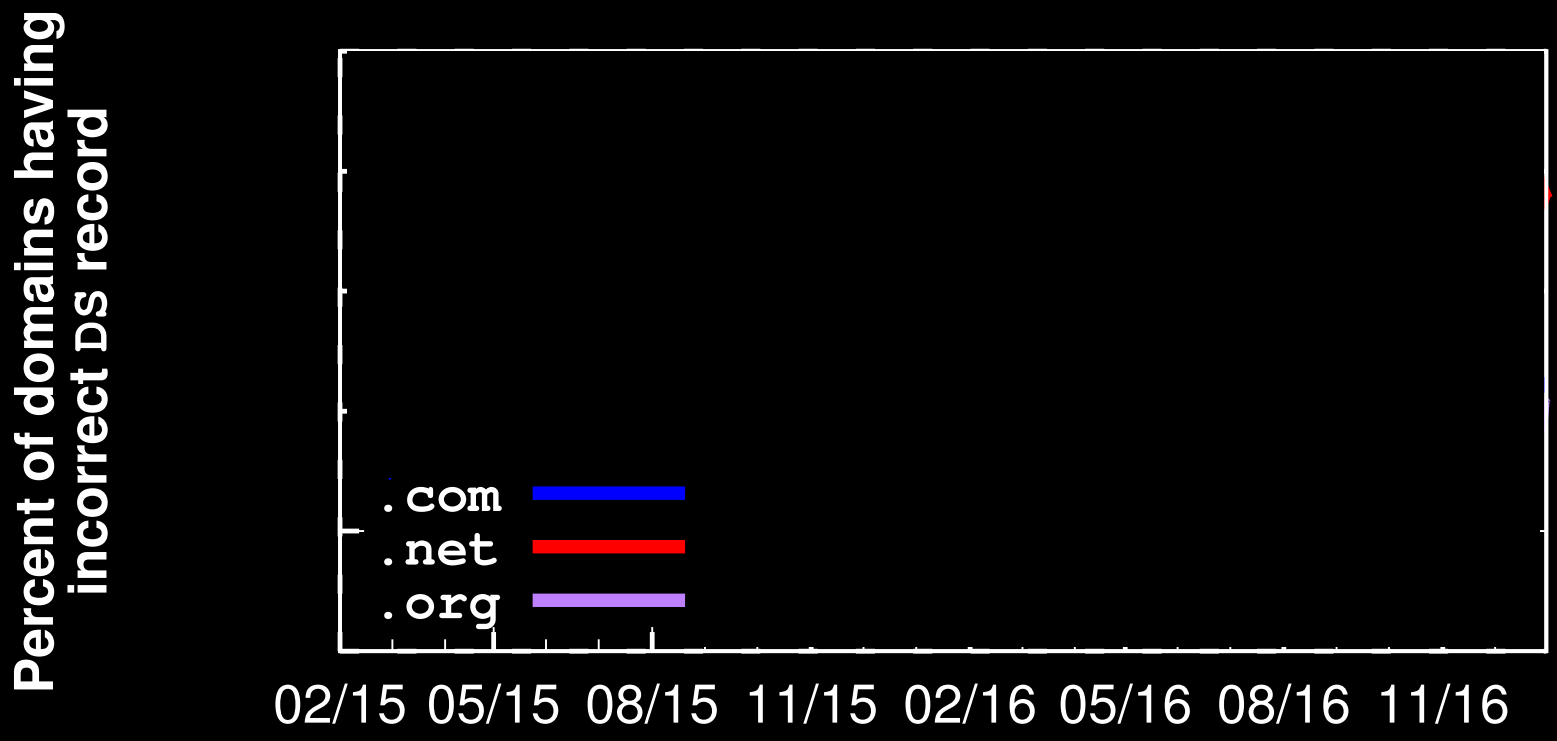
DNSKEY ~1.0%

RRSIGs ~0.3%

Valid RRSIGs ~0.5%

DS record Uploads ~30%

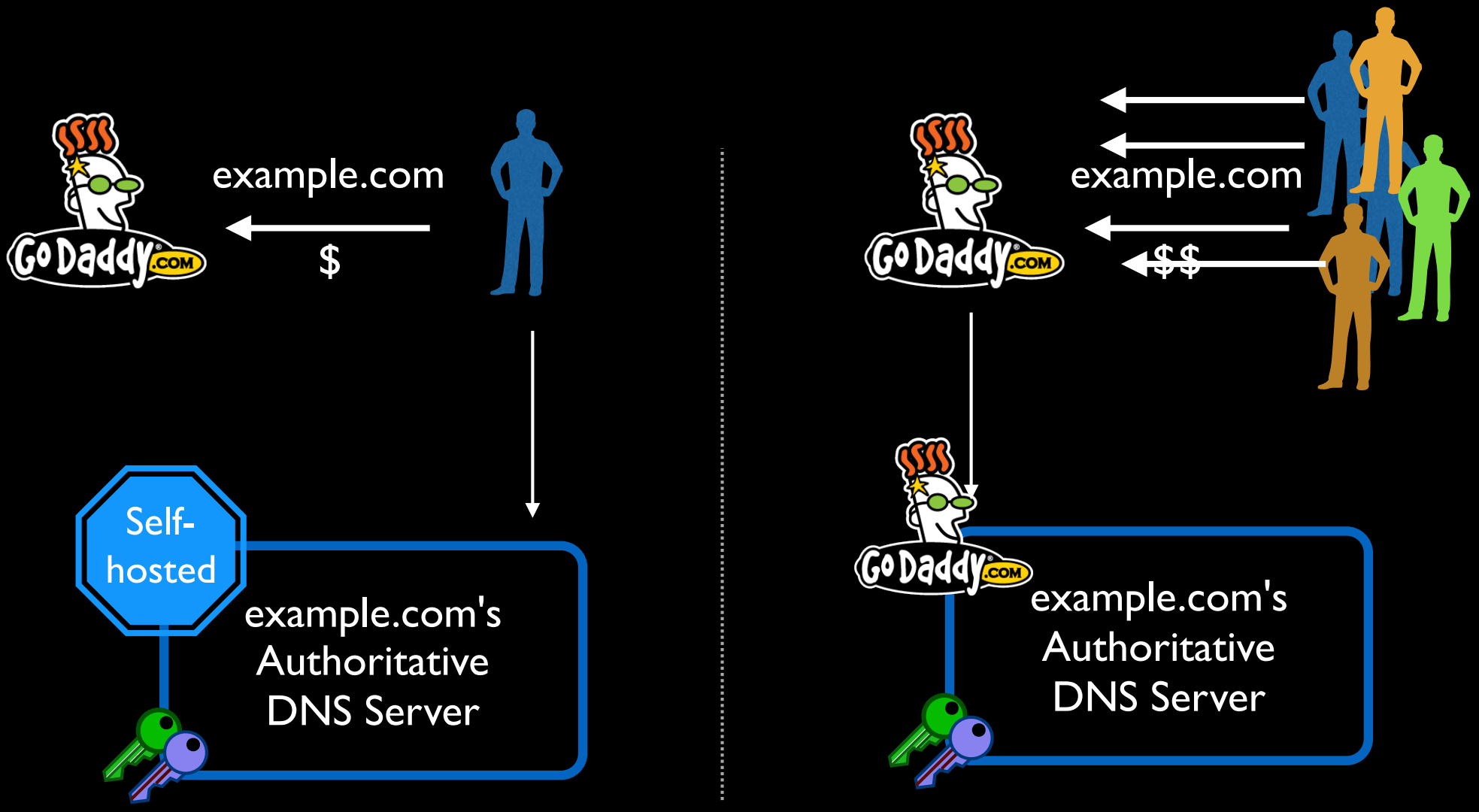
Valid DS record ~0.2%



Incorrect DS record

Once DS record is generated, it is managed very well (~0.2%)

Choosing Authoritative Nameserver



Why are DS records missing?

Nameservers	# of domains		DS Publishing Ratio
	w/ DS	w/ DNSKEY	
ovh.net		316,960	
loopia.se		131,726	
hyp.net		94,084	
transip.net		91,103	
domainmonster.com		60,425	
anycast.me		52,381	
transip.nl		47,007	
binero.se		44,650	
ns.cloudflare.com		28,938	
is.nl		15,738	
pcextreme.nl		14,967	
webhostingserver.nl		14,806	
registrar-servers.com		13,115	
ns0.nl		12,738	
citynetwork.se		11,660	

Why are DS records missing?

Nameservers	# of domains		DS Publishing Ratio
	w/ DS	w/ DNSKEY	
ovh.net	315,204	316,960	99.45%
loopia.se	1	131,726	0.00%
hyp.net	93,946	94,084	99.85%
transip.net	91,009	91,103	99.90%
domainmonster.com	4	60,425	0.01%
anycast.me	51,403	52,381	98.13%
transip.nl	46,971	47,007	99.92%
binero.se	17,099	44,650	38.30%
ns.cloudflare.com	17,483	28,938	60.42%
is.nl	11	15,738	0.07%
pcextreme.nl	14,801	14,967	98.89%
webhostingserver.nl	10,655	14,806	71.96%
registrar-servers.com	11,463	13,115	87.40%
ns0.nl	12,674	12,738	99.50%
citynetwork.se	13	11,660	0.11%

Why are DS records missing?

Nameservers	# of domains		DS Publishing Ratio
	w/ DS	w/ DNSKEY	
ovh.net	315,204	316,960	99.45%
loopia.se	1	131,726	0.00%
hyp.net	93,946	94,084	99.85%
[illegible]	[illegible]	[illegible]	[illegible]
pcextreme.nl	14,801	14,967	98.89%
webhostingserver.nl	10,655	14,806	71.96%
registrar-servers.com	11,463	13,115	87.40%
ns0.nl	12,674	12,738	99.50%
citynetwork.se	13	11,660	0.11%

"Most people do not understand DNS, so imagine the white faces when I mention DNSSEC ... I don't think DNSSEC has a high priority anymore currently in our organization or our customer base."

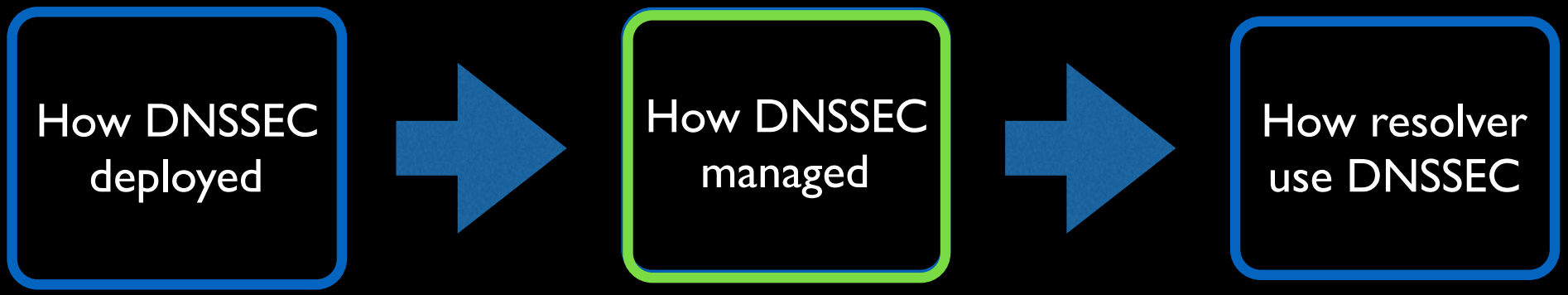
Summary of DNSSEC Deployment

- DNSSEC deployment is still rare, but increasing
- The major reason of broken DNSSEC is due to the missing DS record
  - Missing RRSIG record: ~ 0.3%
  - Incorrect RRSIG record: ~ 0.3 %
  - Incorrect DS record: ~ 0.2%
  - Missing DS Record: ~ 30%

- Most of the DNSSEC-support softwares (BIND, Windows Server 2012, PowerDNS, OpenDNSSEC) manage the keys automatically. Regardless, the process to upload DS record is totally dependent on the administrator!

Outline

30% of domain miss DS records!



Authoritative Server

Resolver

Good Steps to Deploy DNSSEC

(1) Have a cryptographically strong key

(2) Don't reuse across multiple domains

(3) Replace on a regular basis

Good Steps to Deploy DNSSEC

(1) Have a cryptographically strong key

(2) Don't reuse across multiple domains

(3) Replace on a regular basis

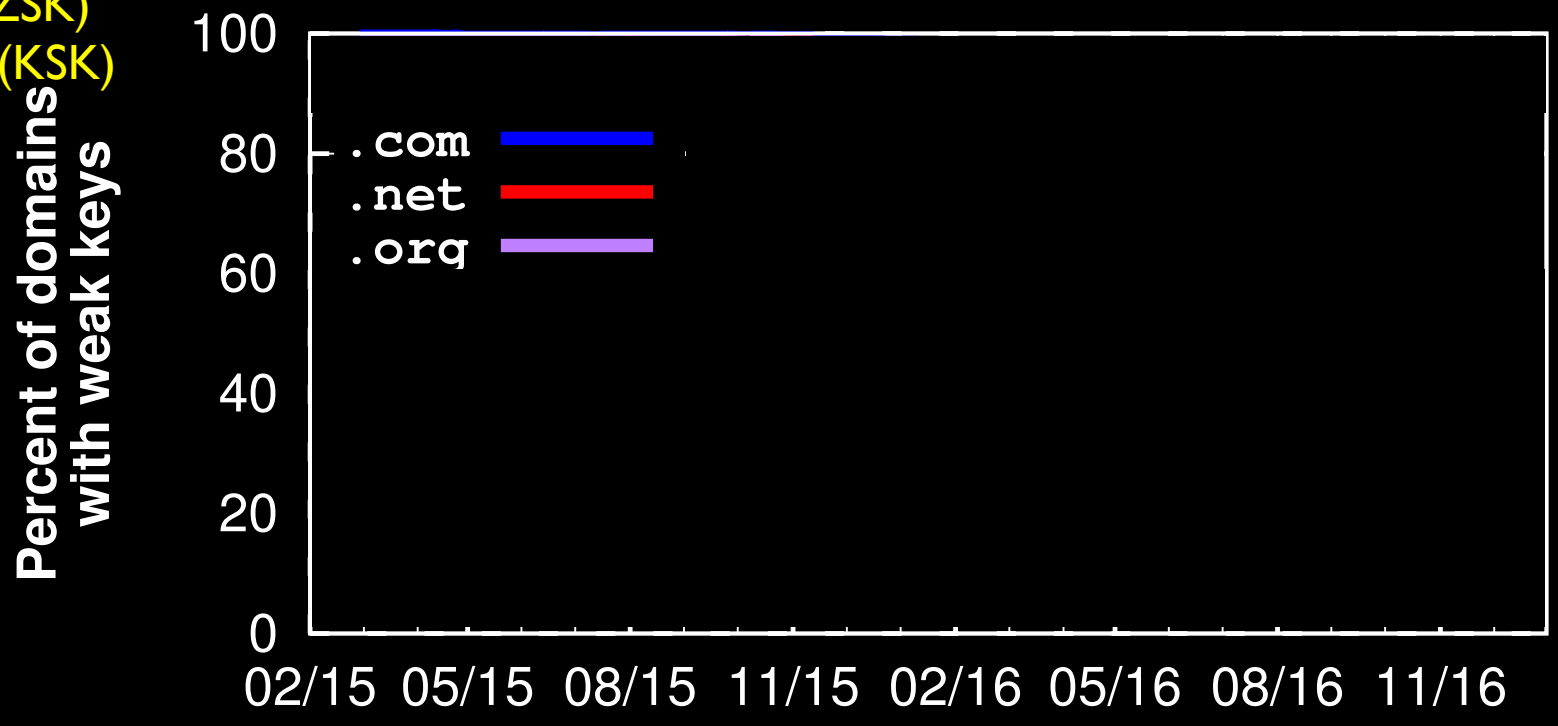
Key Strength

Strong Key

8.3% (ZSK)
66.7% (KSK)

No Reuse

Regular Rollover



Weak Keys

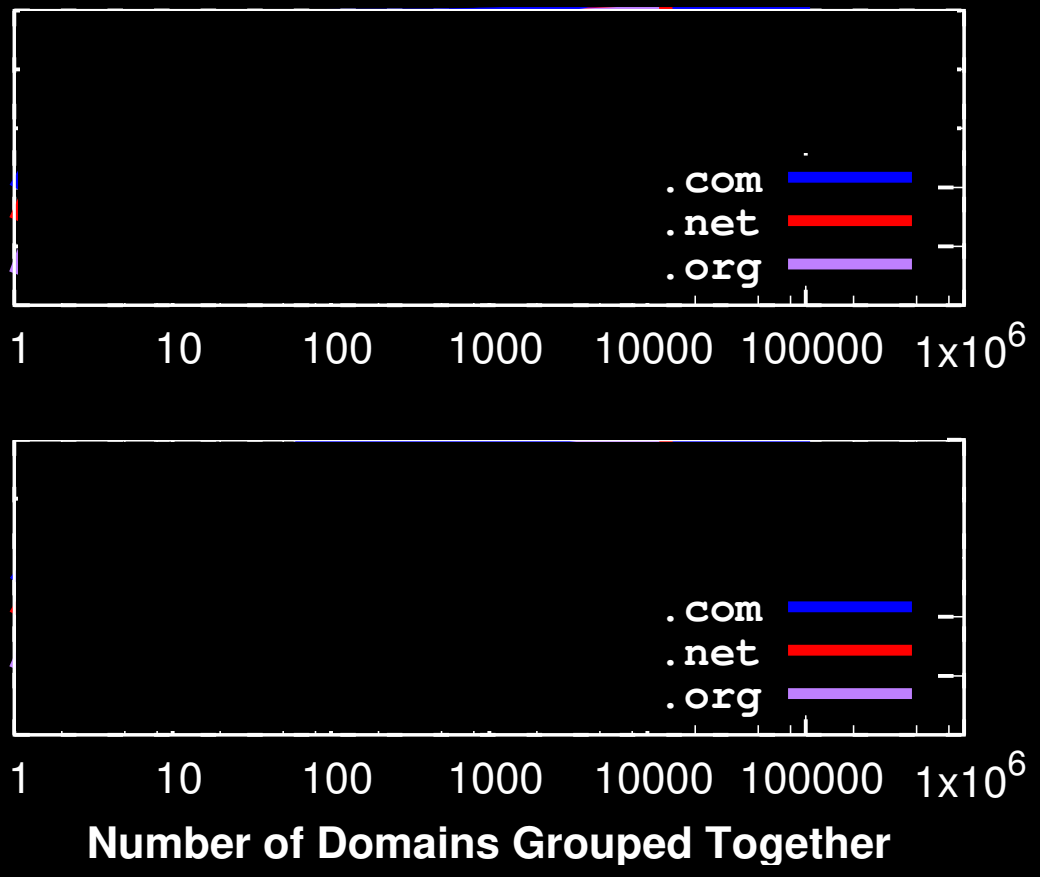
91.7% of ZSK and 33.3% of KSK are weak!

Key Reuse

Strong Key — 91.7% (ZSK), 33.3% (KSK)

No Reuse — ~0.1%

Regular Rollover — 45.0% (ZSK), 70.0% (KSK)



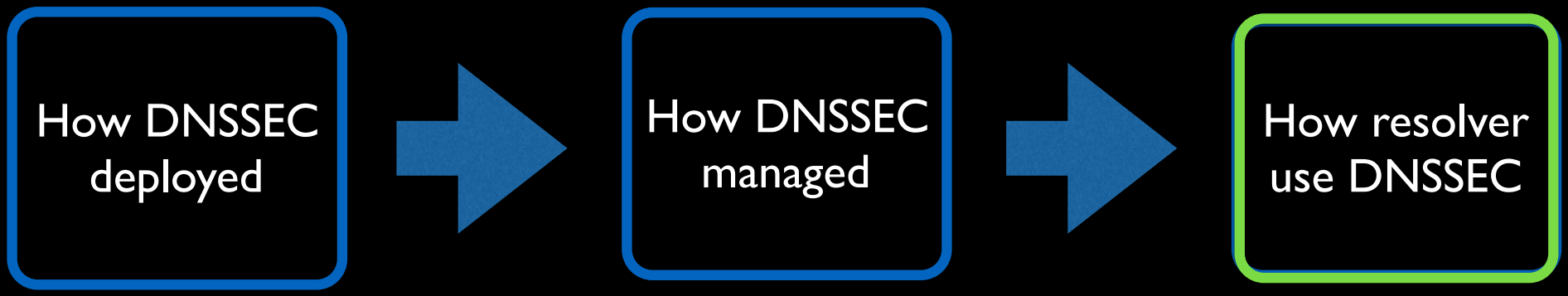
DNSKEY Sharing

Some keys are reused extensively (among 106,640 domains)

Outline

30% of domain miss DS records!

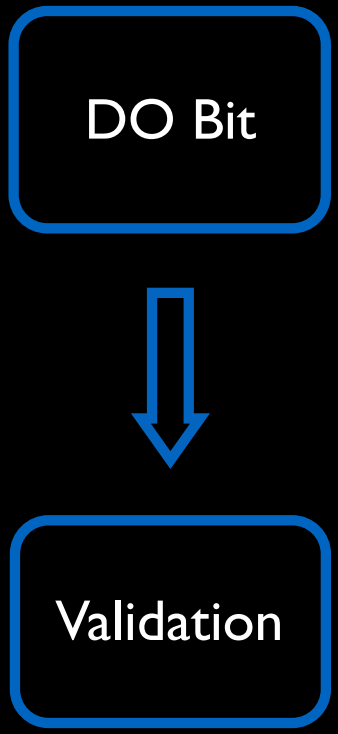
33% weak
45~70% not switched



Authoritative Server

Resolver

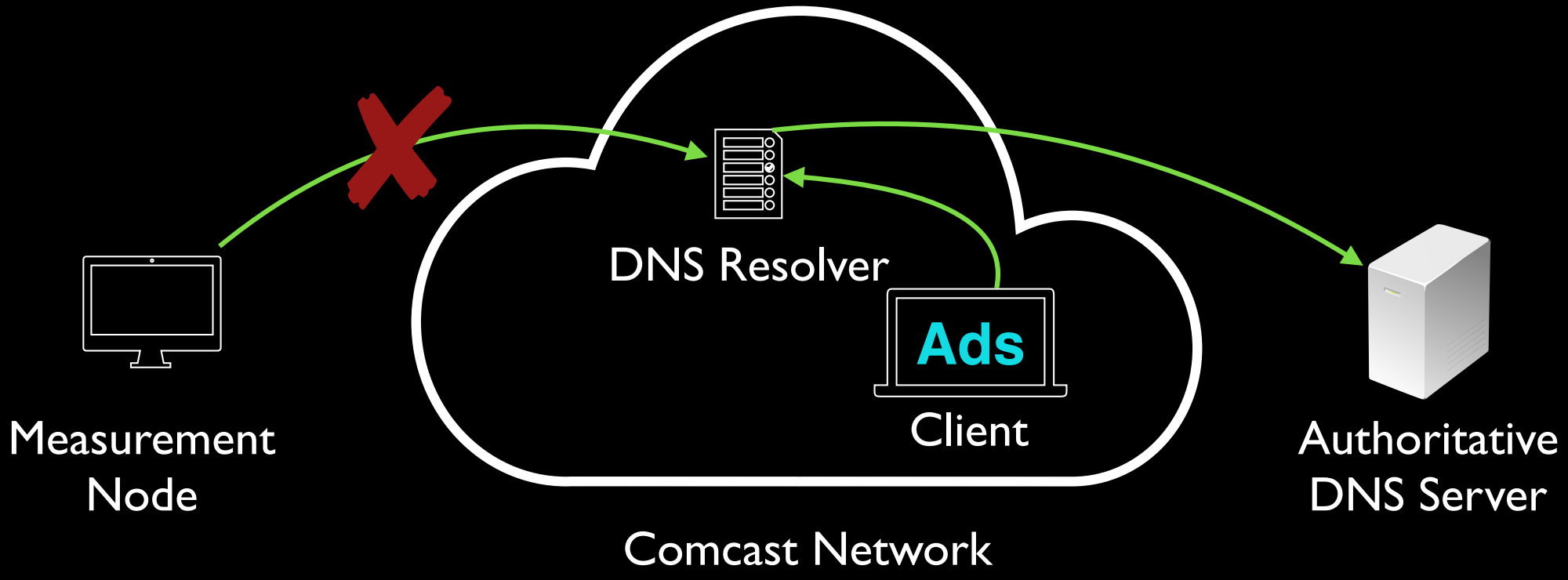
Correct Deployment for Resolvers



(1) DNSSEC OK bit in the header

(2) Validate DNSSEC Records

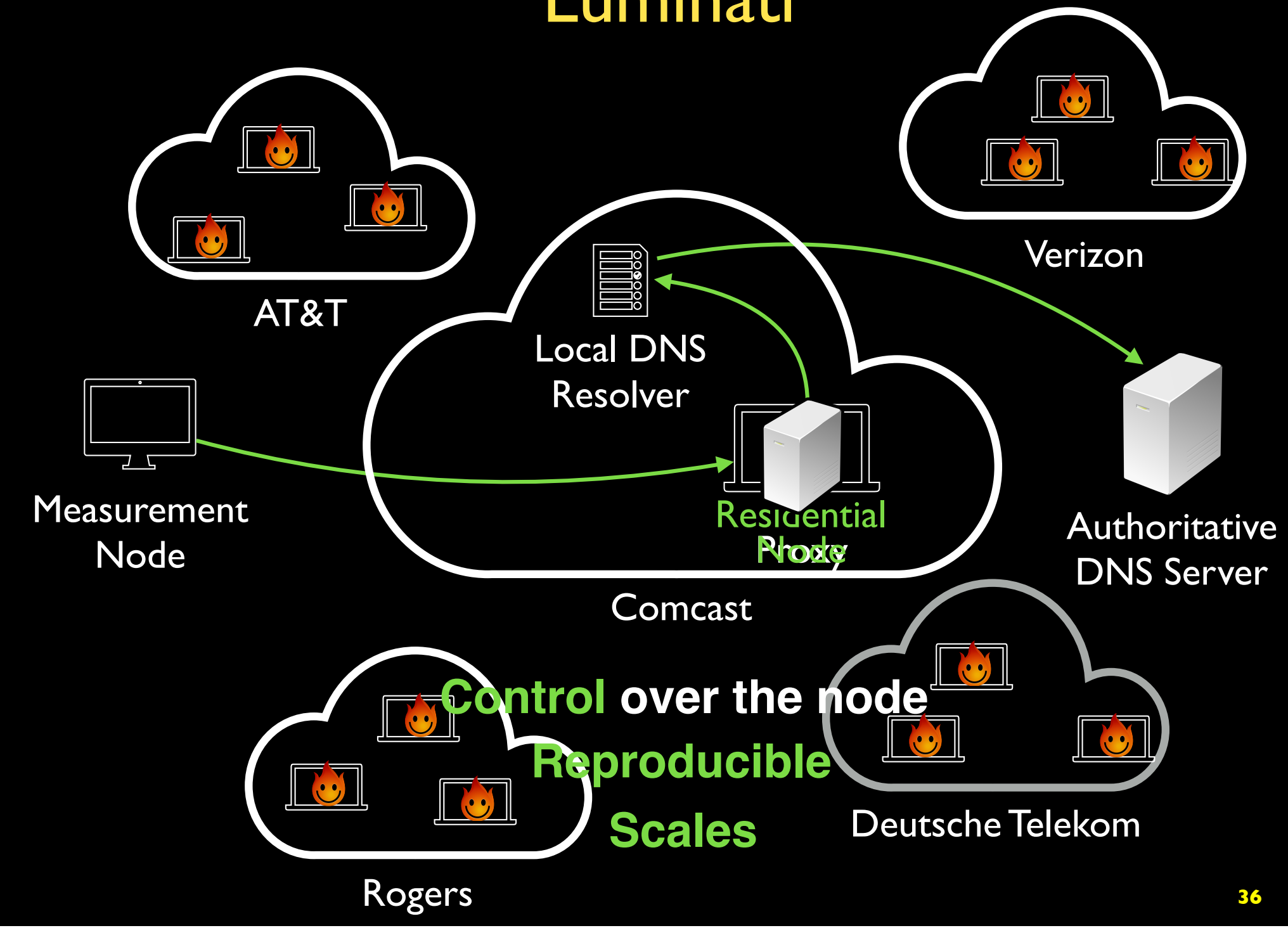
Measuring DNS resolver



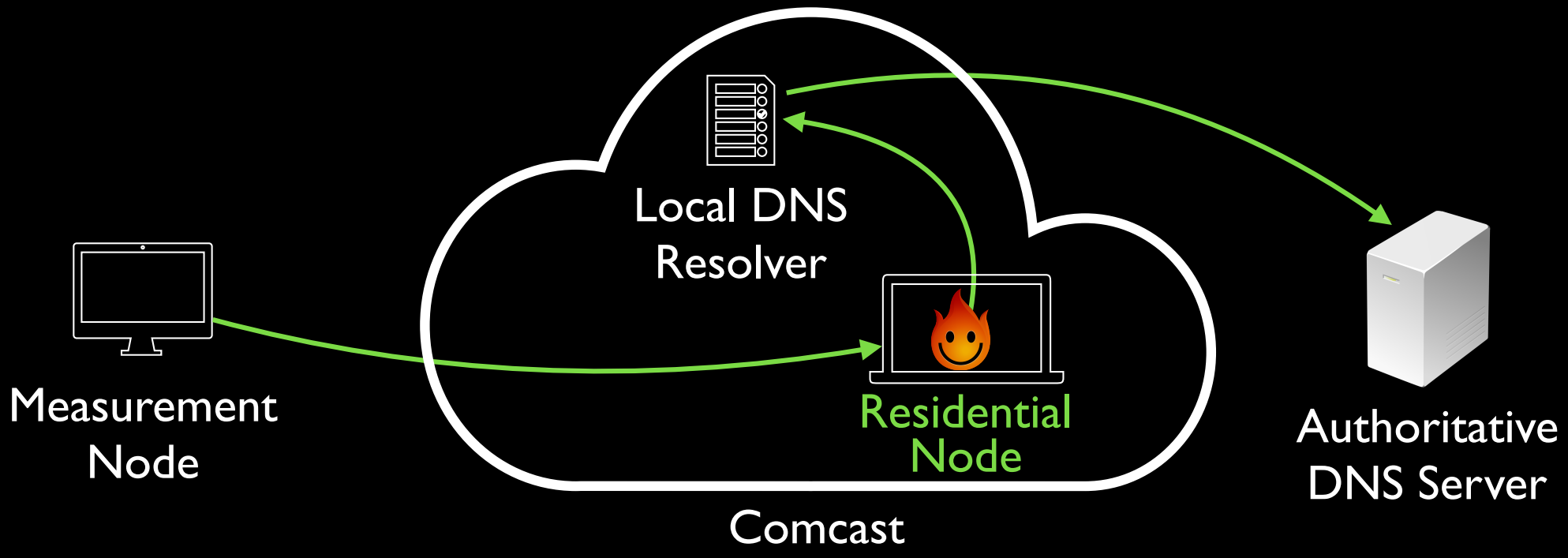
No Control over the node

Not Reproducible

Luminati


AT&T
Verizon
Local DNS Resolver
Measurement Node
Residential Node
Authoritative DNS Server
Comcast
Control over the node
Reproducible
Scales
Rogers
Deutsche Telekom

Luminati



Control over the node

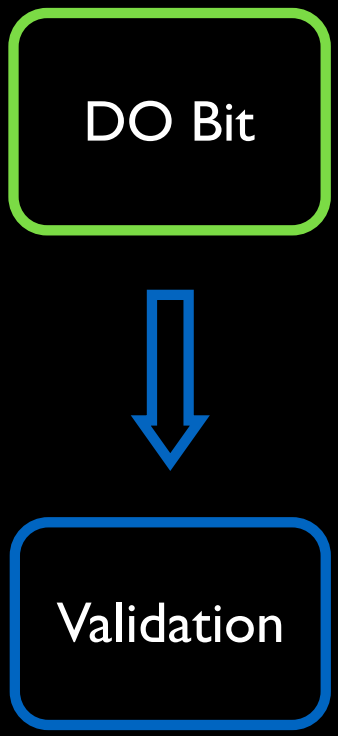
Reproducible

Scales

Methodology

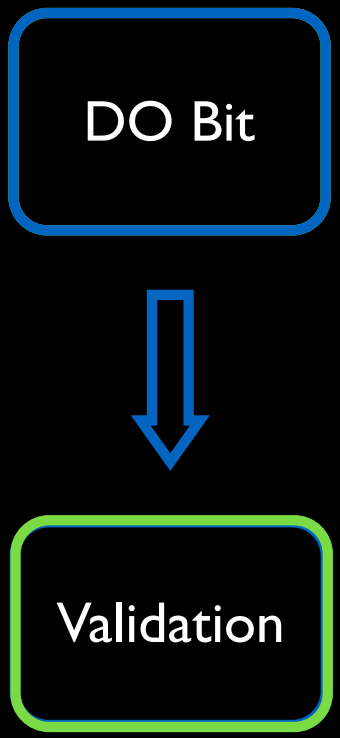
+ 8 other scenarios of incorrect DNSSEC records

Resolvers w/ DO Bit



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

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

Conclusion

- Presented a longitudinal, end-to-end study of DNSSEC ecosystem
- DNSSEC deployment from server-side is rare but growing
  - ✓ But, 33% of them are mis-configured
  - ✓ DNSKEYs are not managed well
    - ✓ Weak
    - ✓ Some are shared
    - ✓ Rarely updated
- DNSSEC deployment from client-side is also rare
  - ✓ Only 12% of resolvers validate responses
- Datasets and source code will be available.
  - http://securepki.org

Recommendations

- Use CDS (Child DS) / CDNSKEY (Child DNSKEY)
  - Automates DNSSEC delegation trust maintenance
- Modern resolvers (e.g., BIND >= 9.5) set "DO" bit by default, but make sure that it actually validates.
- Financial incentives for registrars to deploy DNSSEC would work
  - .se and .nl ccTLD
  - Please read our upcoming paper "*Understanding the Role of Registrars in DNSSEC Deployment* [IMC'17]"

Conclusion

- Presented a longitudinal, end-to-end study of DNSSEC ecosystem
- DNSSEC deployment from server-side is rare but growing
  - ✓ But, 33% of them are mis-configured
  - ✓ DNSKEYs are not managed well
    - ✓ Weak
    - ✓ Some are shared
    - ✓ Rarely updated
- DNSSEC deployment from client-side is also rare
  - ✓ Only 12% of resolvers validate responses
- Datasets and source code will be available.
  - http://securepki.org

Questions?

Why DNSSEC Deployment is so Low?

"Understanding the Role of Registrars in DNSSEC Deployment" [IMC'17]

Ethical Consideration

Subject	Considration
Luminati	Paid for access
	Not violate ToS
Exit Nodes	Not expose PII
	Connects only our testbed
	Download "Empty" Page

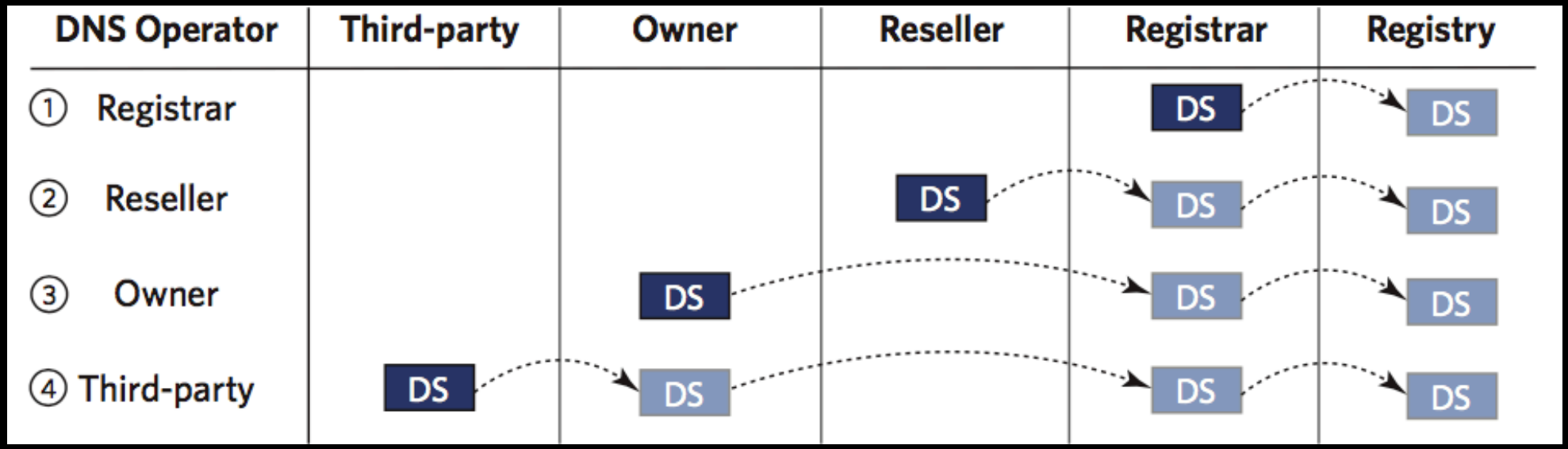
Scenario and Intuition

subdomains	description	requires DS	requires DNSKEY
missing-rrsig-a	no signature for A record	0	0
invalid-rrsig-a	invalid signature for A record	0	1
future-rrsig-a	signature is not yet valid	0	0
past-rrsig-a	signature is expired	0	0
missing-zsk	ZSK used to sign A record is not in DNSKEY	0	1
missing-ksk	KSK used to sign DNSKEY record is not in DNSKEY	0	1
missing-rrsig-ksk	no signature for DNSKEY record	0	1
invalid-rrsig-ksk	invalid signature for DNSKEY record	0	1
mismatch-ds	DS record at parent zone is not accord with KSK	1	1

Structure of Domain Name

- Registry: organizations that manage top-level domains (TLDs). They maintain the TLD *zone file* (the list of all registered names), and work with registrars to sell domain names to the public.
  - Verisign
- Registrar: organizations that are accredited by ICANN[3] and certified by registries to sell domains to the public. They have direct access to the registry.
  - GoDaddy
- Reseller: organizations that sell domain names, but are either not accredited (by ICANN) or certified (by a given TLD's registry). Typically, resellers partner with registrars in order to sell domain names, and relay all information through the registrar.

DS record uploads



Key Sharing

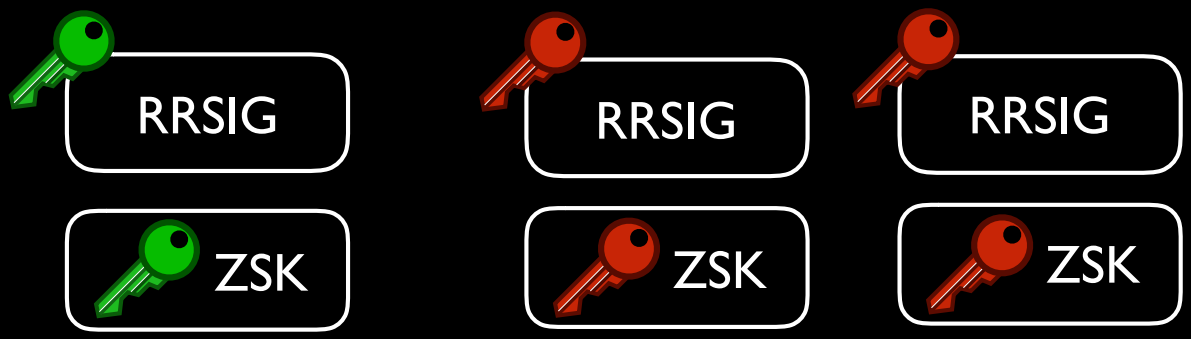
Nameservers	KSK		ZSK	
	Keys	Domains	Keys	Domains
Others		151,733		152,144
ovh.net.		316,888		316,887
loopia.se.		133,258		133,258
hyp.net.		94,888		94,885
transip.net.		93,819		93,818
domainmonster.com.		60,984		60,984
anycast.me.		55,936		55,936
transip.nl.		45,676		45,675
binero.se.		44,963		44,963
ns.cloudflare.com.		28,469		28,469
is.nl.		12,837		12,836
pcextreme.nl.		15,210		15,210
webhostingserver.nl.		15,023		15,023
registrar-servers.com.		13,183		13,181
ns0.nl.		11,945		11,945
citynetwork.se.		11,702		11,702

Key Sharing

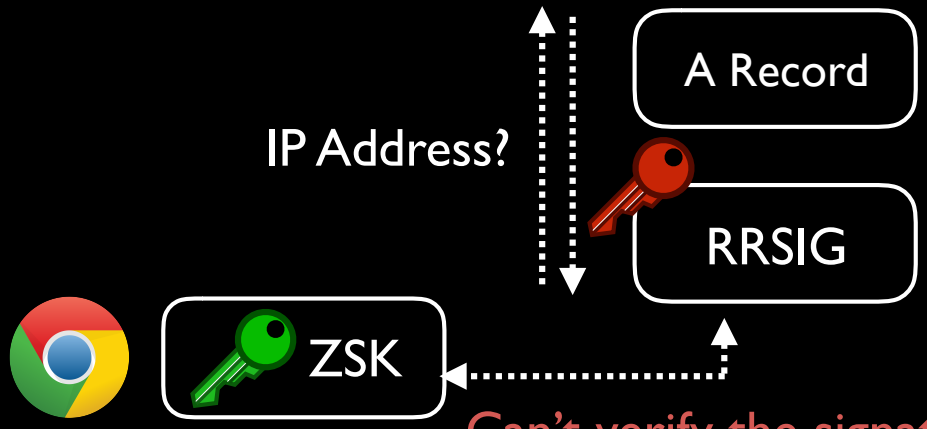
Nameservers	KSK		ZSK	
	Keys	Domains	Keys	Domains
Others	157,533	151,733	188,482	152,144
ovh.net.	318,036	316,888	326,011	316,887
loopia.se.	199	133,258	217	133,258
hyp.net.	119,150	94,888	119,161	94,885
transip.net.	93,774	93,819	187,129	93,818
domainmonster.com.	60,991	60,984	121,939	60,984
anycast.me.	56,075	55,936	58,296	55,936
transip.nl.	45,648	45,676	91,161	45,675
binero.se.	49	44,963	54	44,963
ns.cloudflare.com.	239	28,469	214	28,469
is.nl.	12,834	12,837	25,512	12,836
pcextreme.nl.	15,192	15,210	28,654	15,210
webhostingserver.nl.	15,019	15,023	22,741	15,023
registrar-servers.com.	13,043	13,183	12,998	13,181
ns0.nl.	11,978	11,945	23,790	11,945
citynetwork.se.	21	11,702	28	11,702

Rollover
Abrupt Changes

TTL = 3600

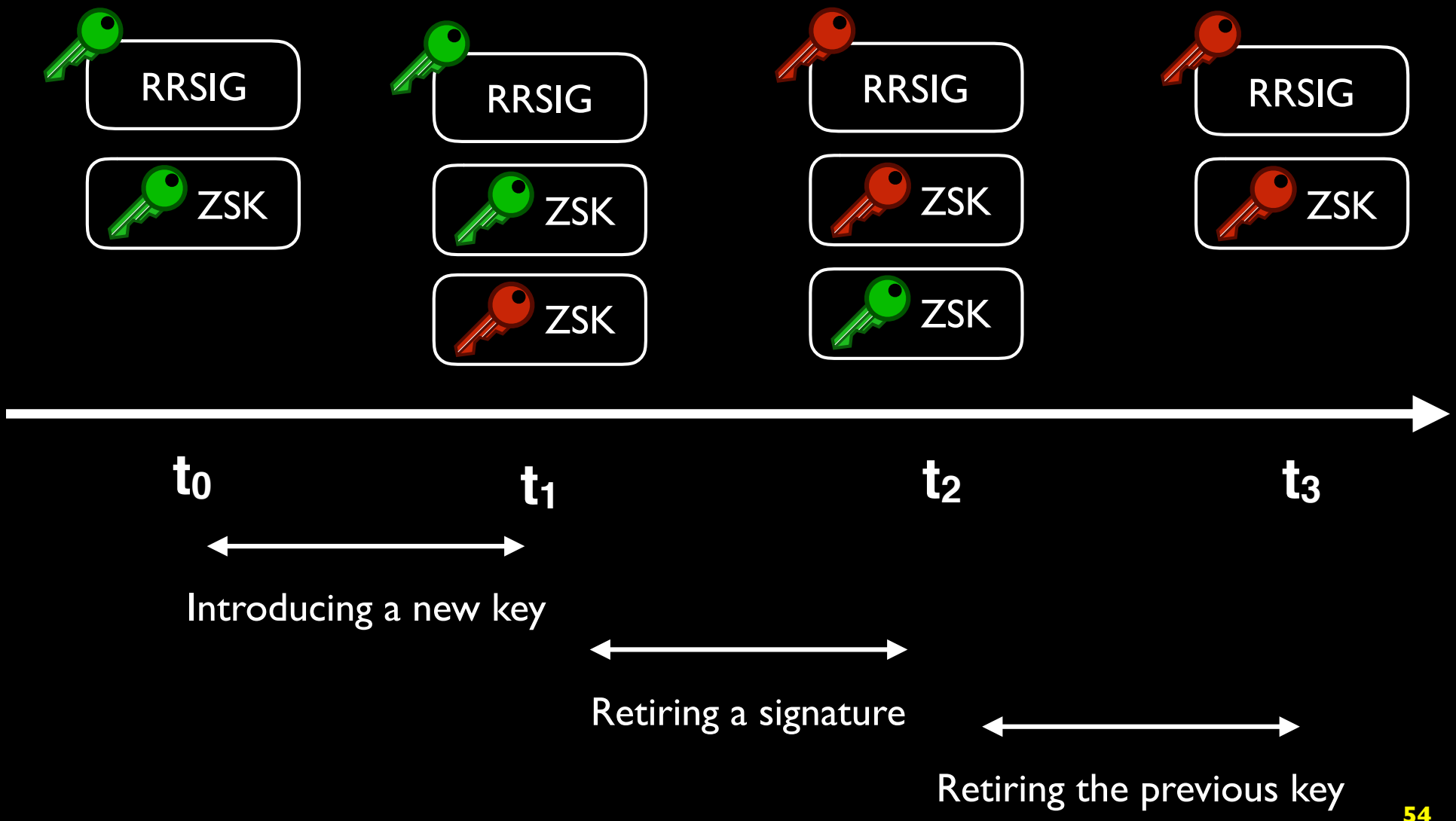


t_0 **$t_0 + 1200$** **$t_0 + 1800$**

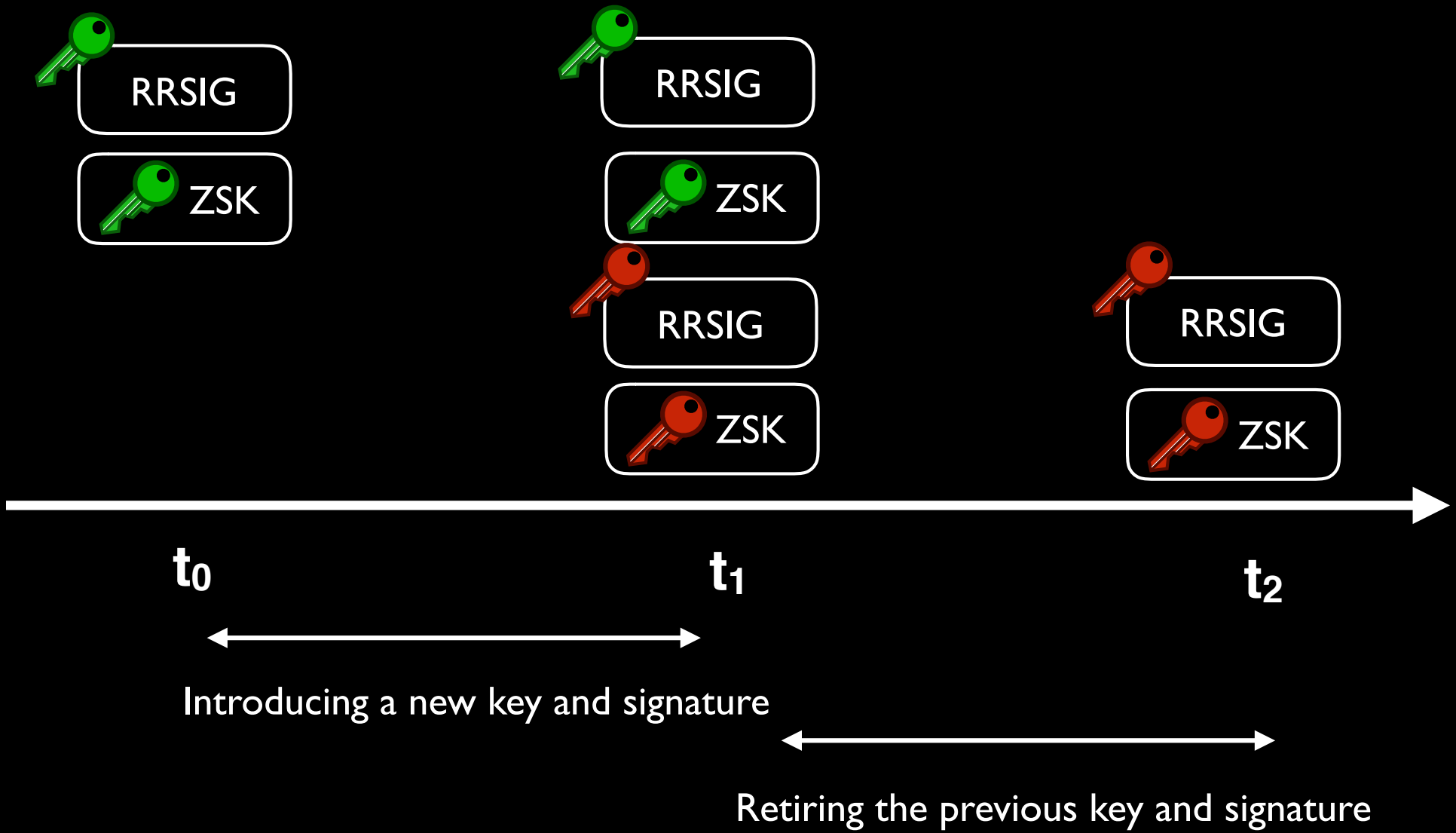


Can't verify the signature!

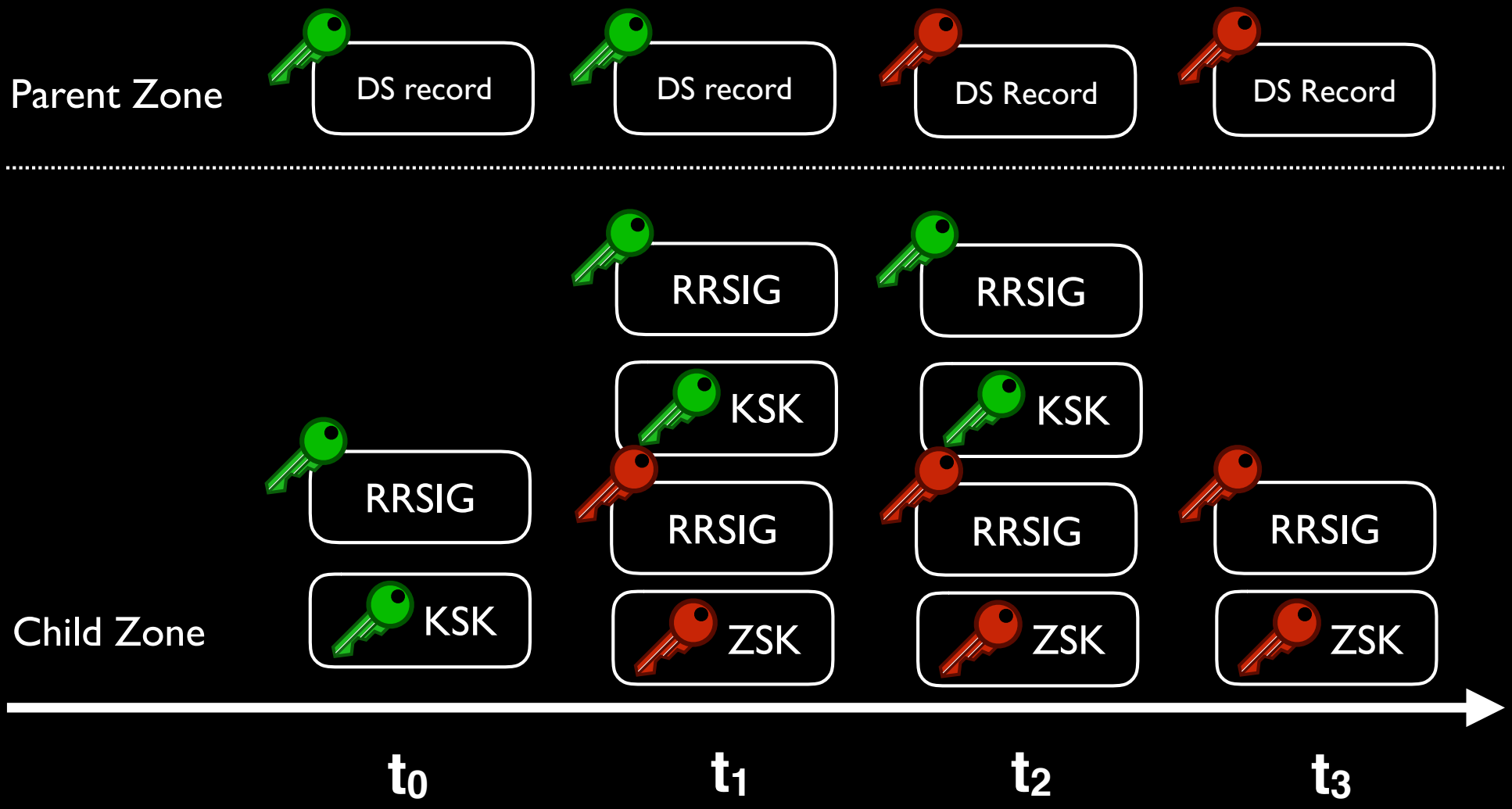
Rollover Process (ZSK)
<Pre-publish>



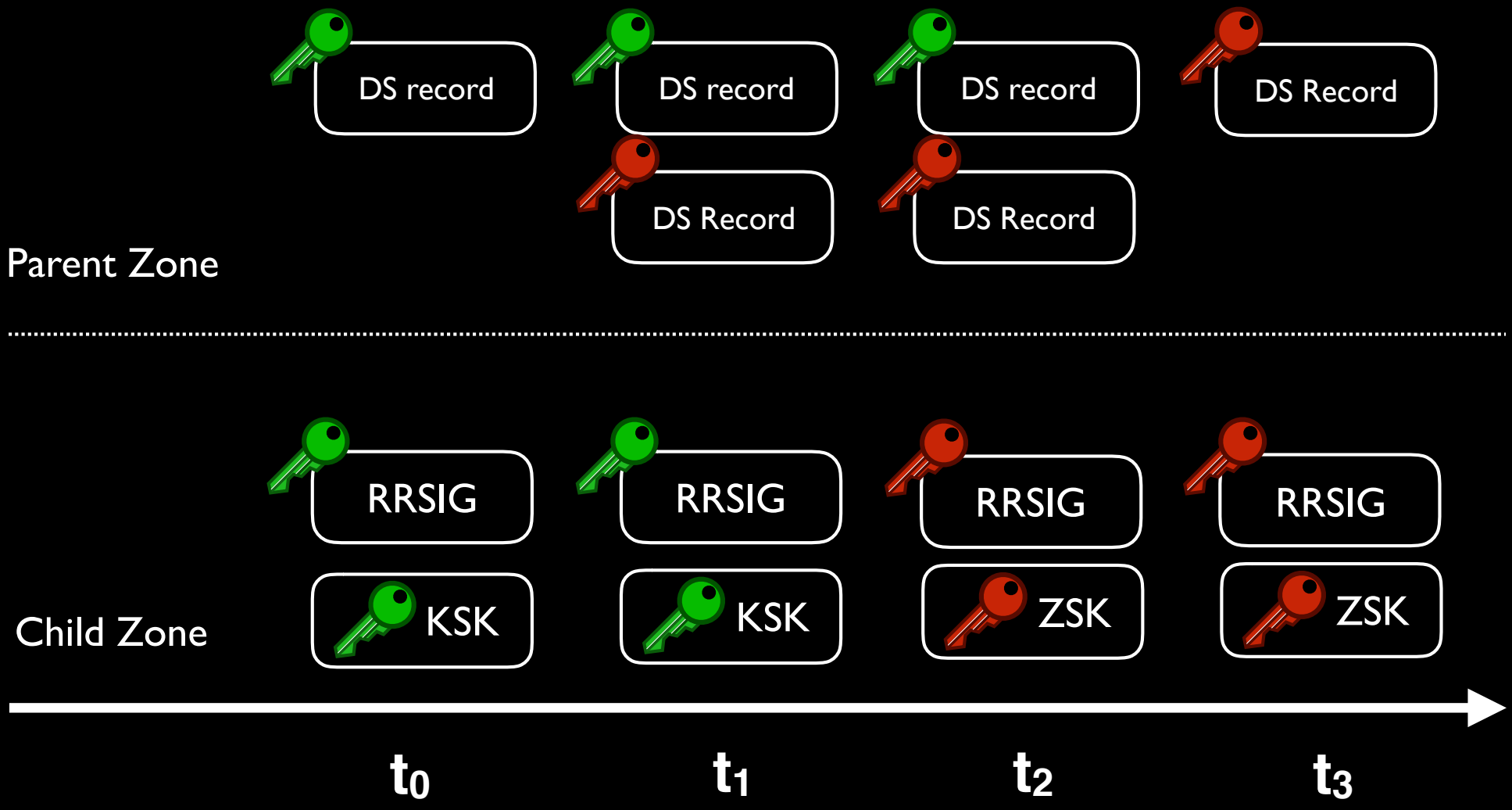
Rollover Process (ZSK)
<Double-signature>



Rollover Process (KSK)
<Double-signature>



Rollover Process (KSK)
<Double-DS>



ZSK Rollovers

Scheme	.com	.org
No ZSK Rollovers	279,935	27,166
Abrupt	5,527	66
Double Signatures	58,807	9,615
Pre-publish	259,327	33,518

ZSK Rollovers

Scheme	.com	.org
No ZSK Rollovers	279,935	27,166
Abrupt	5,527	66
Double Signatures	58,807	9,615
Pre-publish	259,327	33,518

DNSKEY (ZSK)

Nearly 45% of domains DO NOT switch their DNSKEYs

KSK Rollovers

Scheme	.com	.net	.org
No KSK Rollovers	621,213	93,558	65,704
Abrupt	17,724	3,183	1,710
Double Signatures	219,547	46,092	32,206

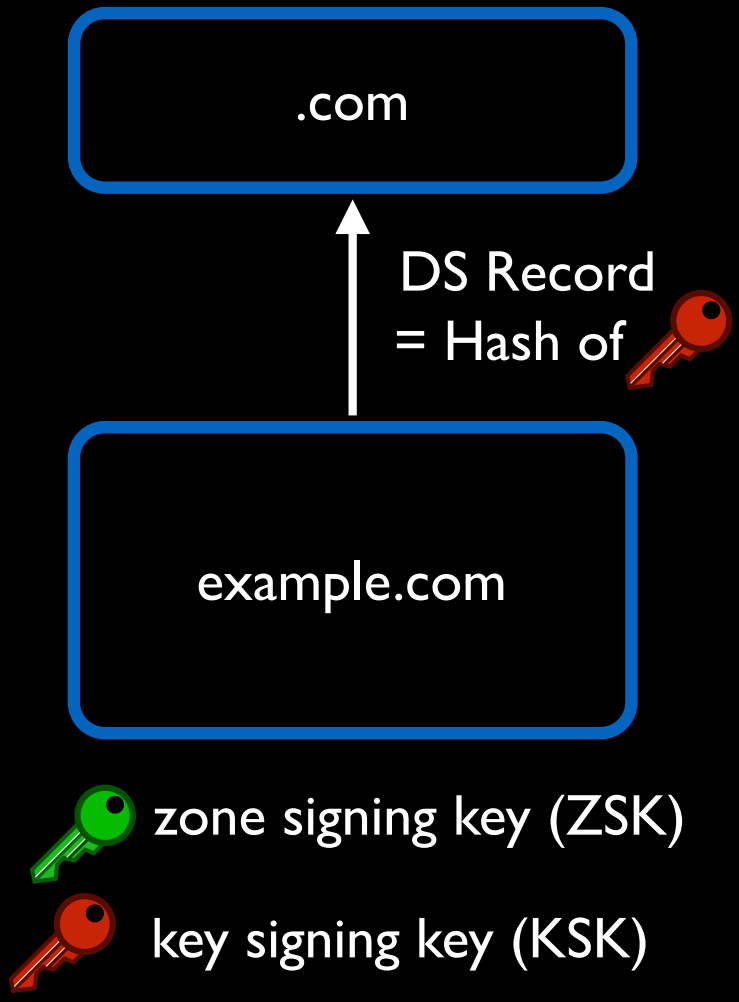
KSK Rollovers

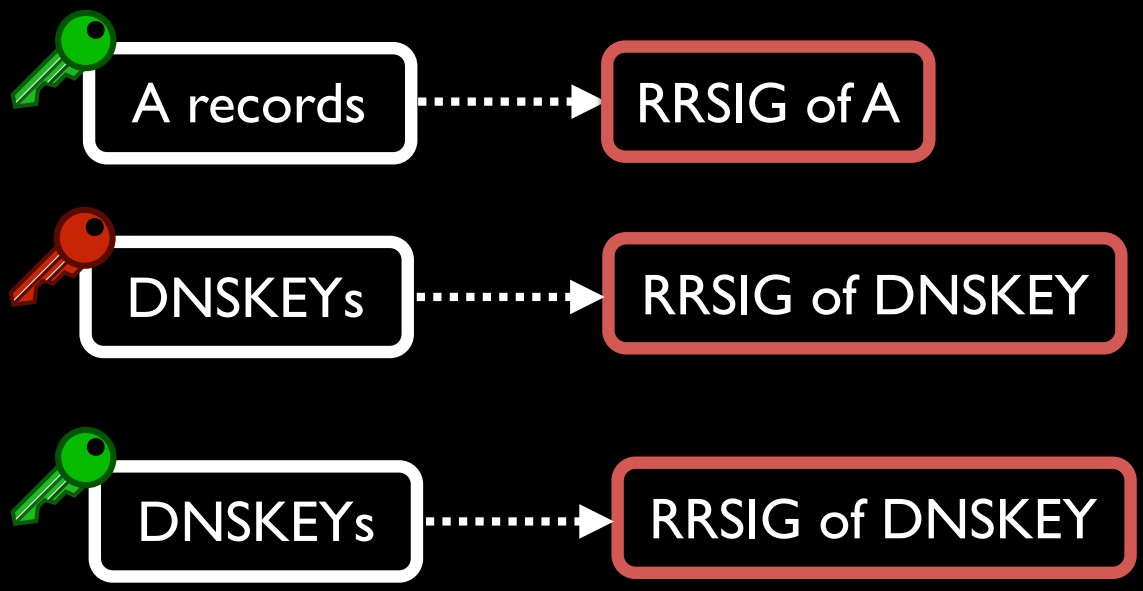
Scheme	.com	.net	.org
No KSK Rollovers	621,213	93,558	65,704
Abrupt	17,724	3,183	1,710
Double Signatures	219,547	46,092	32,206

DNSKEY (KSK)

Nearly 70% of domains DO NOT switch their DNSKEYs

Superfluous Signatures

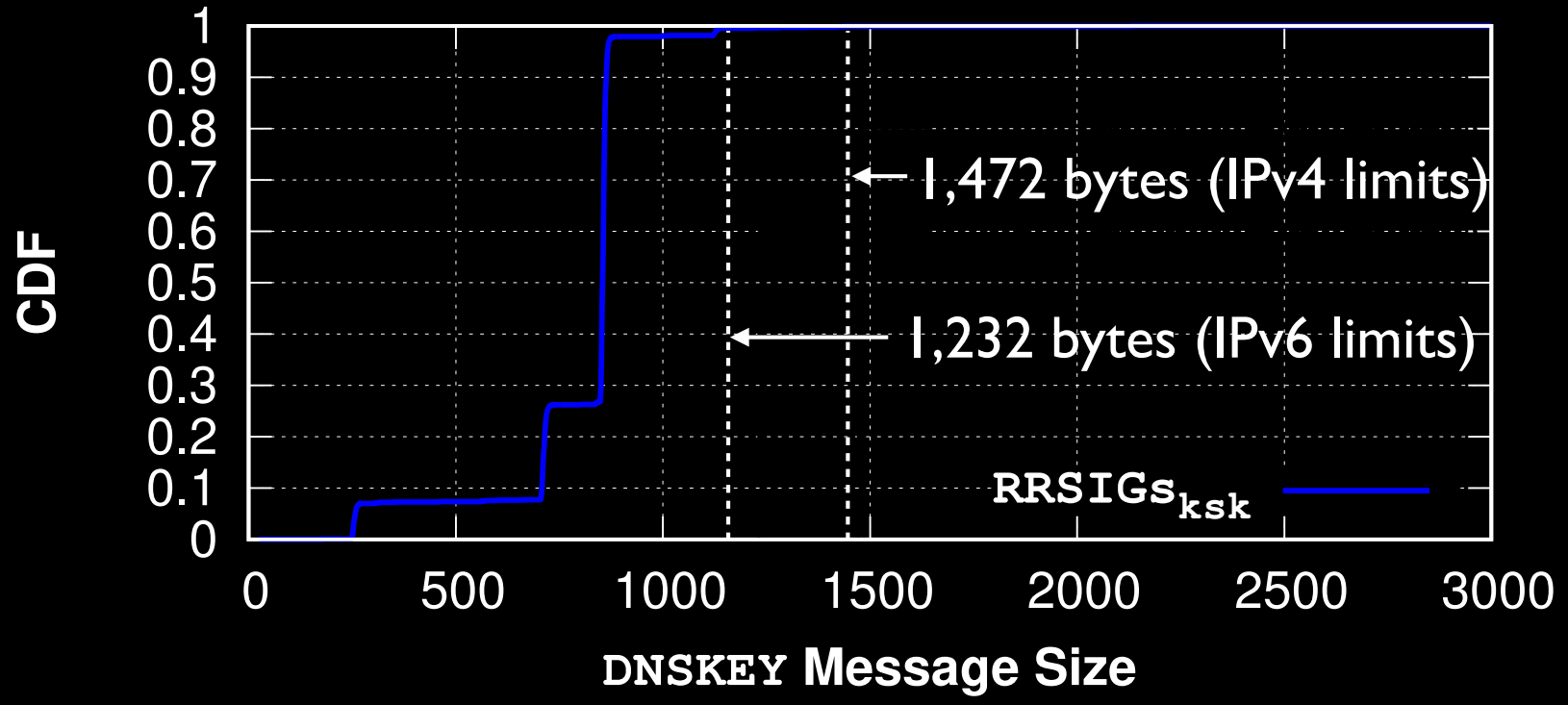




Unnecessary, but not evil!

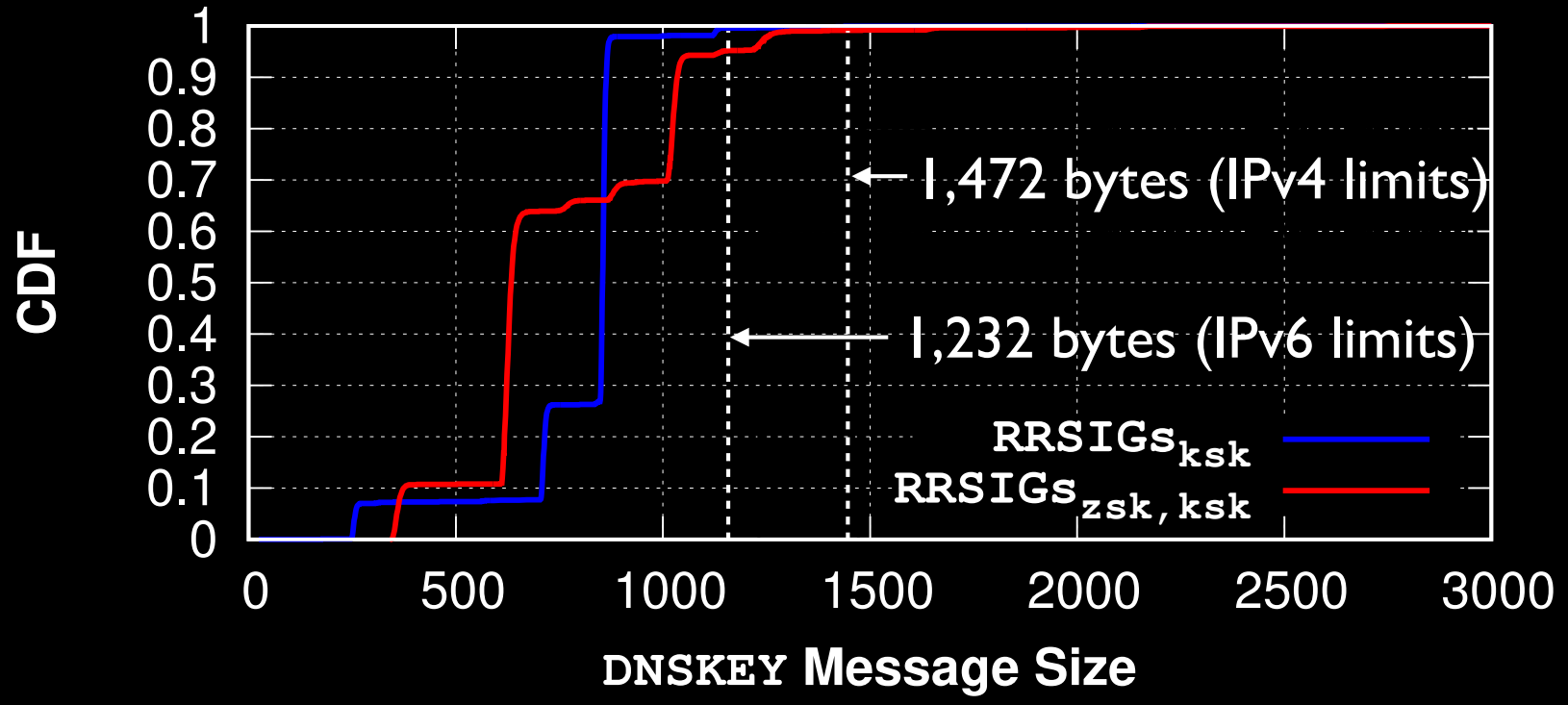
61% of domains sign their DNSKEY twice!
so what?

DNSKEY Fragmentation



0.01% experience fragmentation

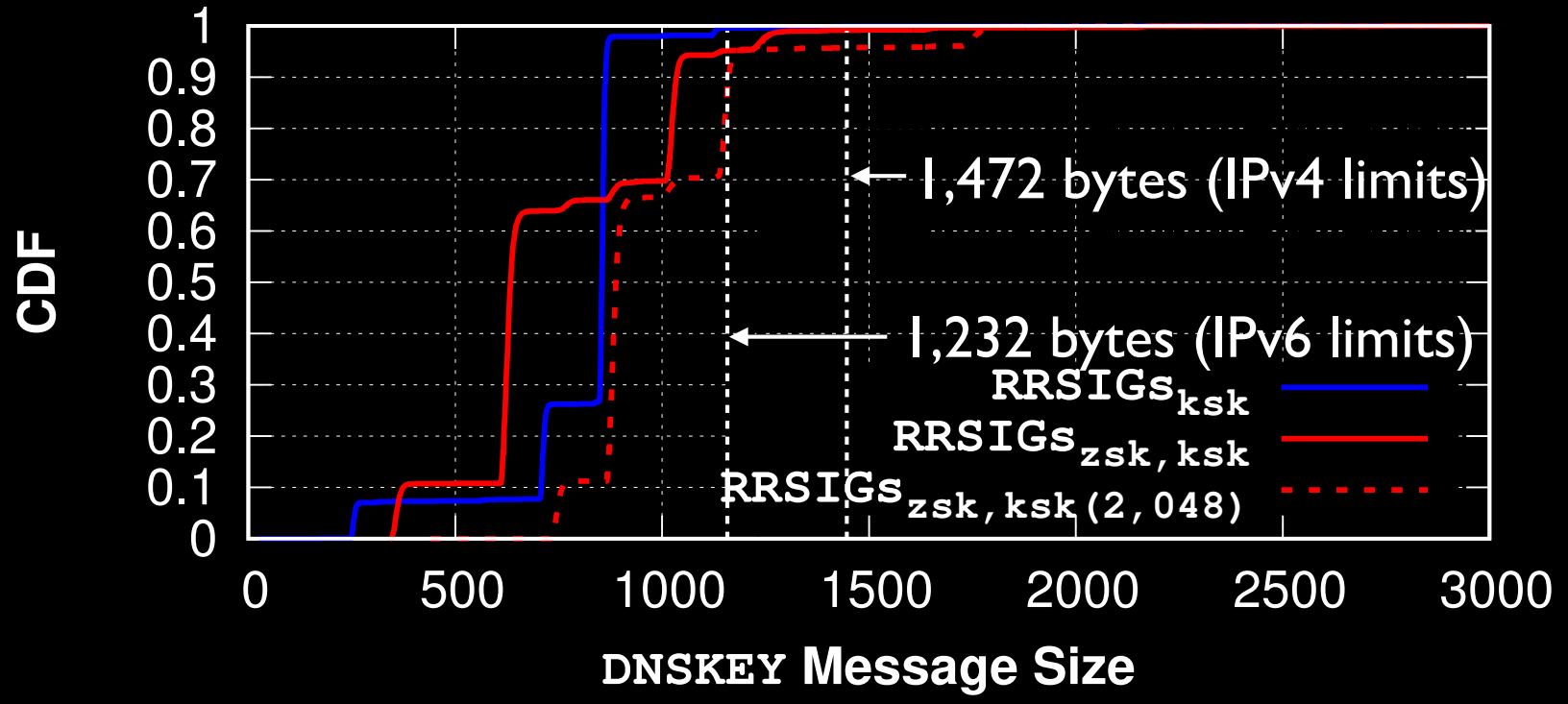
DNSKEY Fragmentation



0.8% experience fragmentation

60.7% of them could have avoided fragmentation

DNSKEY Fragmentation

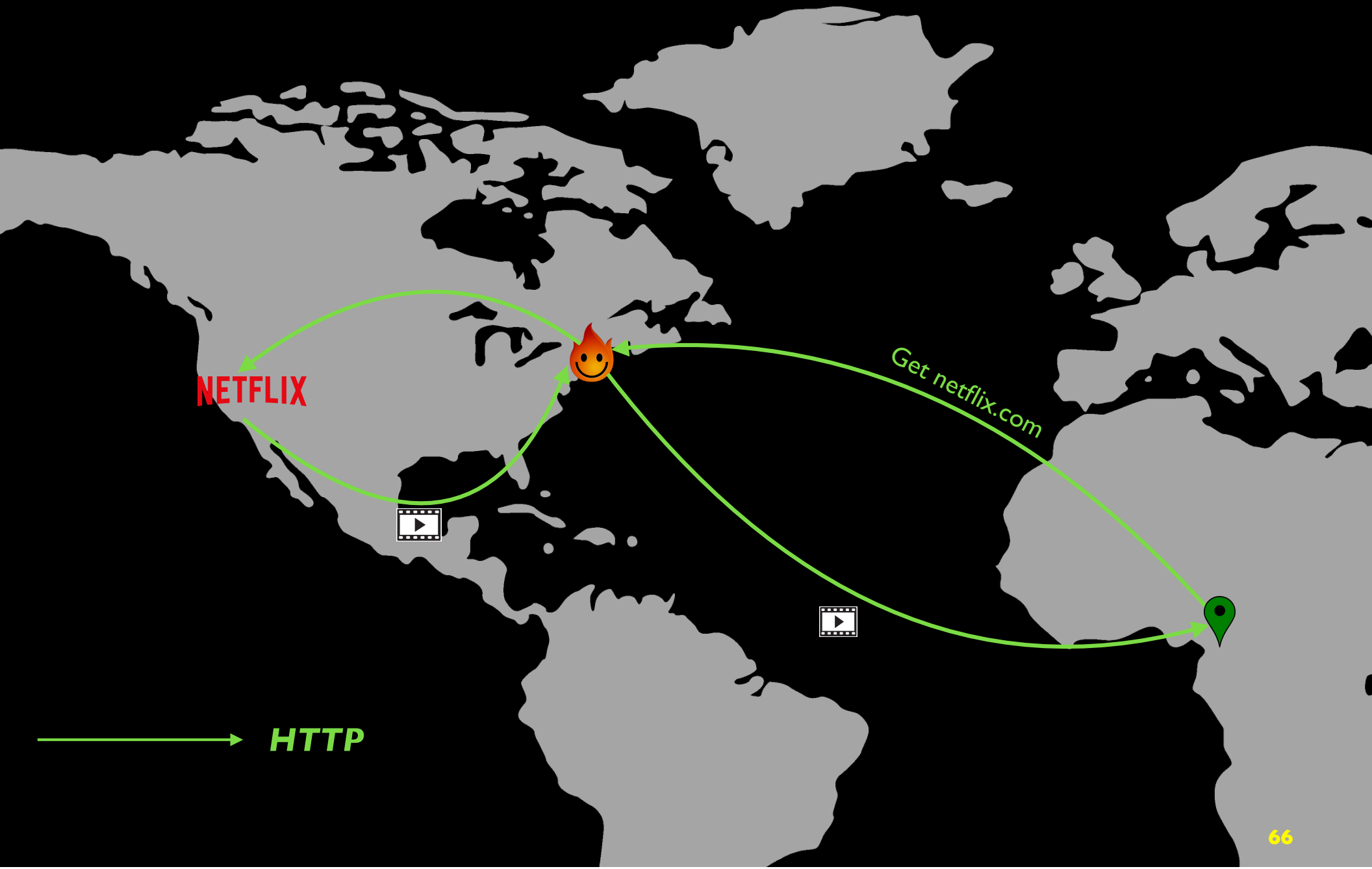


4.6% experience fragmentation (increased 5x times)

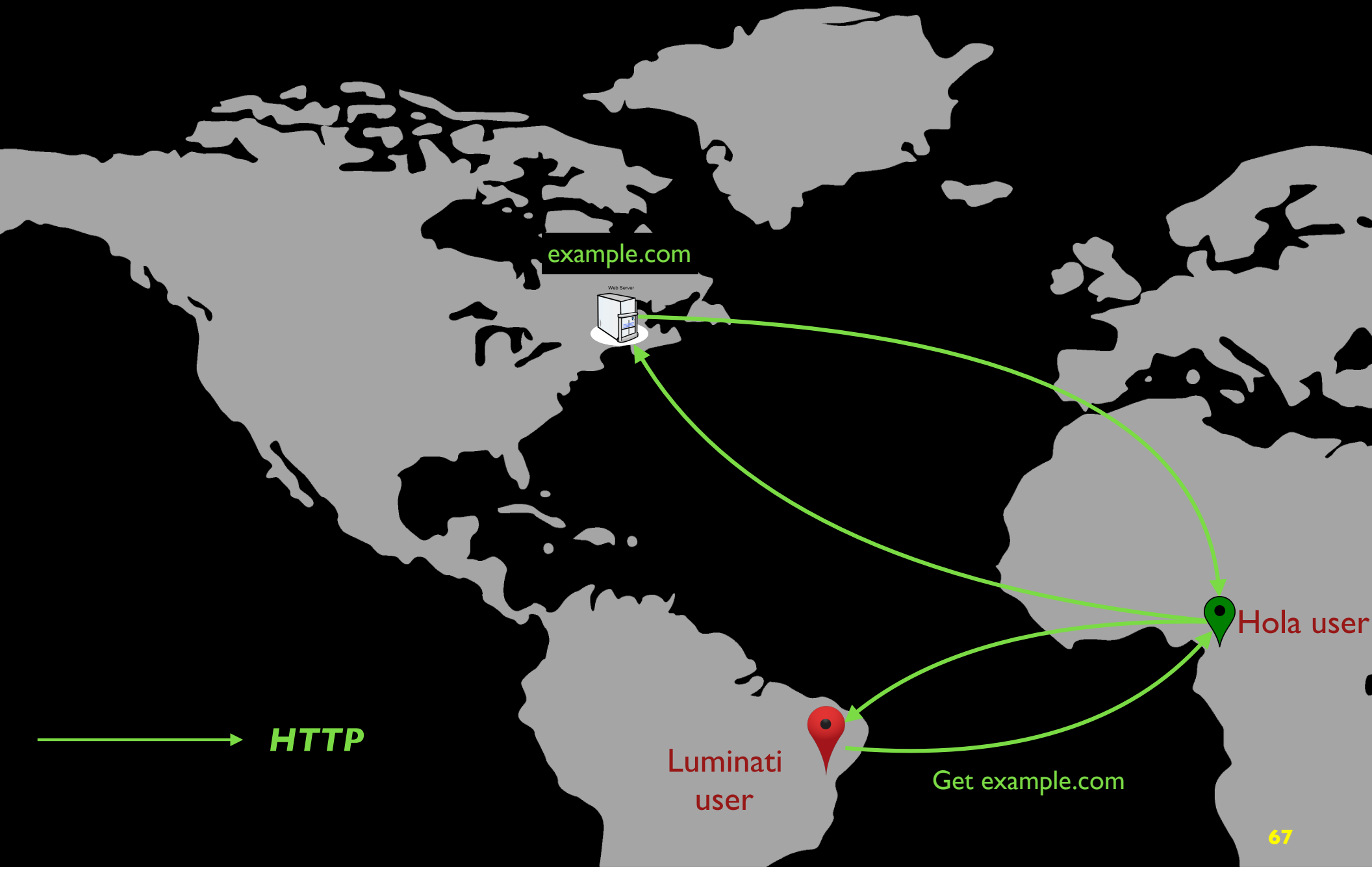
DNSKEY Fragmentation

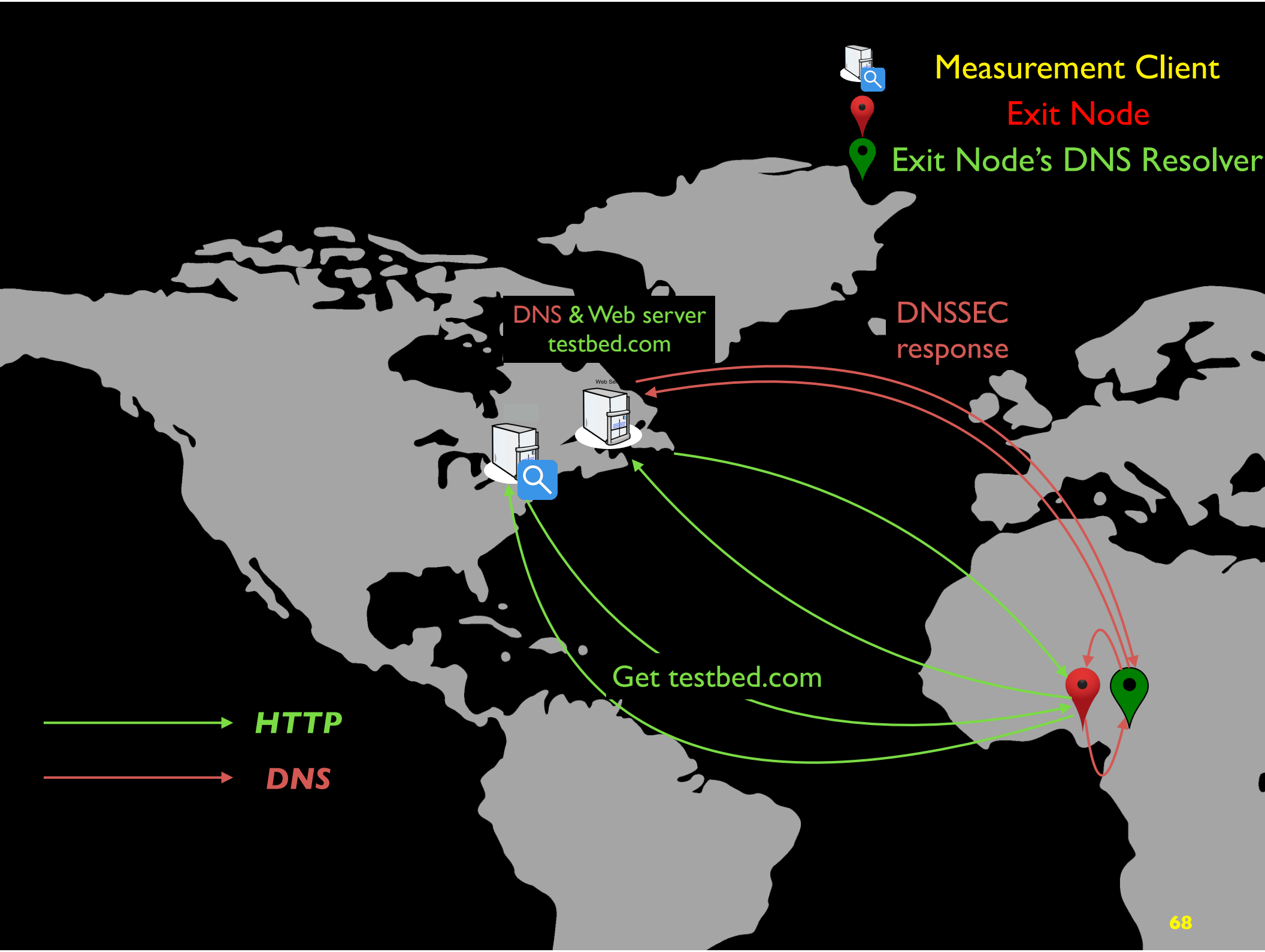
Superfluous signatures increases the chance of fragmentation.

Hola Unblocker

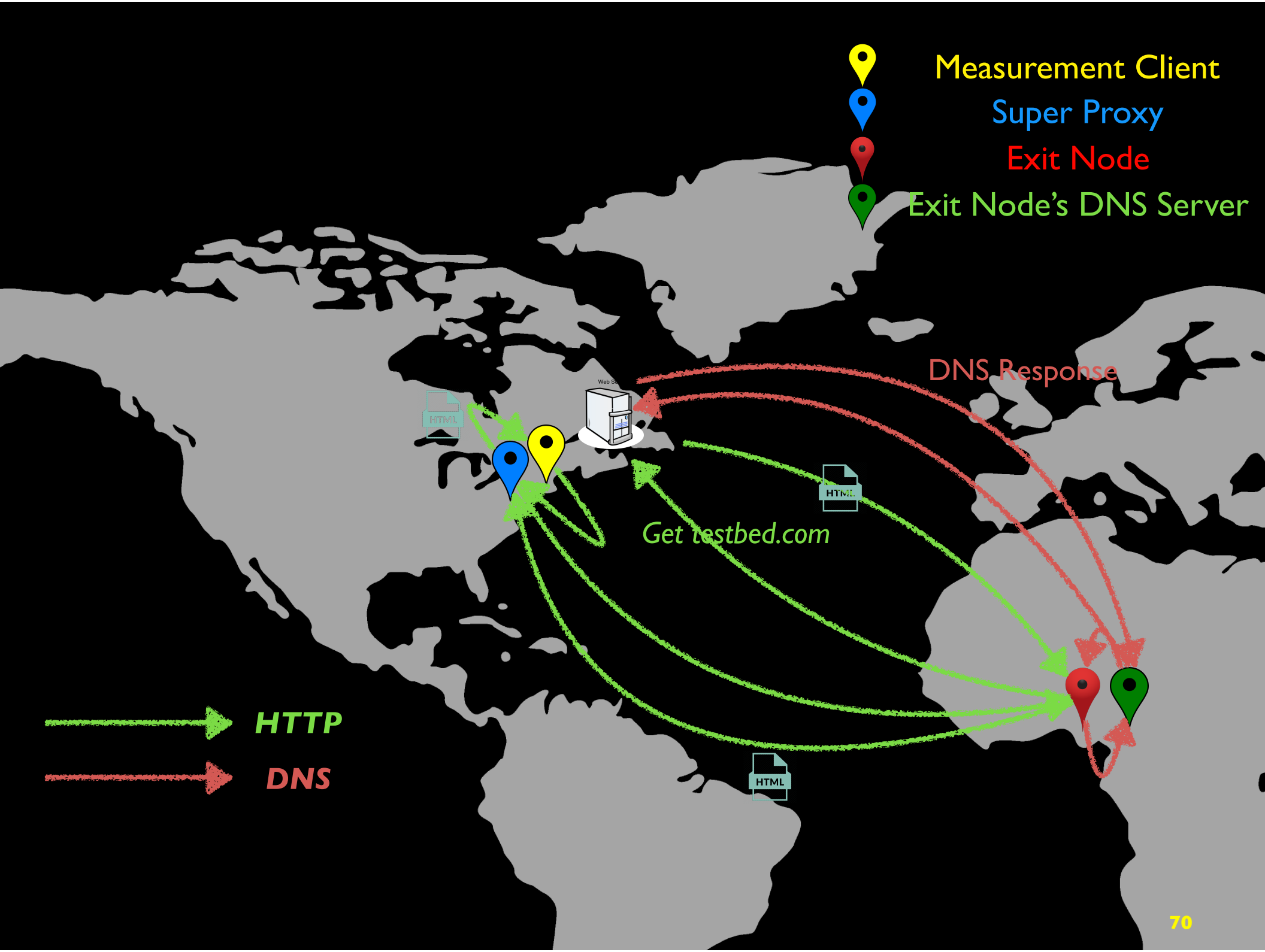


Hola Luminati




Measurement Client
Exit Node
Exit Node's DNS Resolver
DNS & Web server
testbed.com
DNSSEC
response
Get testbed.com
HTTP
DNS


We measured 403,355 nodes
and their 59,513 resolvers !


Measurement Client
Super Proxy
Exit Node
Exit Node's DNS Server
DNS Response
HTML
HTML
HTML
Get testbed.com
HTTP
DNS