Verisign's Transition to Elliptic Curve DNSSEC

Duane Wessels, Verisign

DNS-OARC 42

February 8, 2024

Preparations

- Old algorithm: RSA/SHA-256
  - Algorithm number 8
  - Also known as “RSA”
- New algorithm: Elliptic Curve Digital Signature Algorithm Curve P-256 with SHA-256
  - Algorithm number 13
  - Also known as “ECDSA”
- Began planning early 2023
- Extensive QA and OTE testing
- Fully hands-off design, with changes scheduled at specific times
- Weekly coordination meetings involving multiple teams and 35+ people

Concern: Scheduling

- Rollovers require strict sequencing of events
- Nearly all DNSSEC rollover incidents are due to scheduling mistakes
  - Signatures without corresponding keys
  - DS records without corresponding signatures
- Solutions:
  - Conservative double-signing
  - Automated scheduling
  - Extensive testing

Concern: Resolution Failures

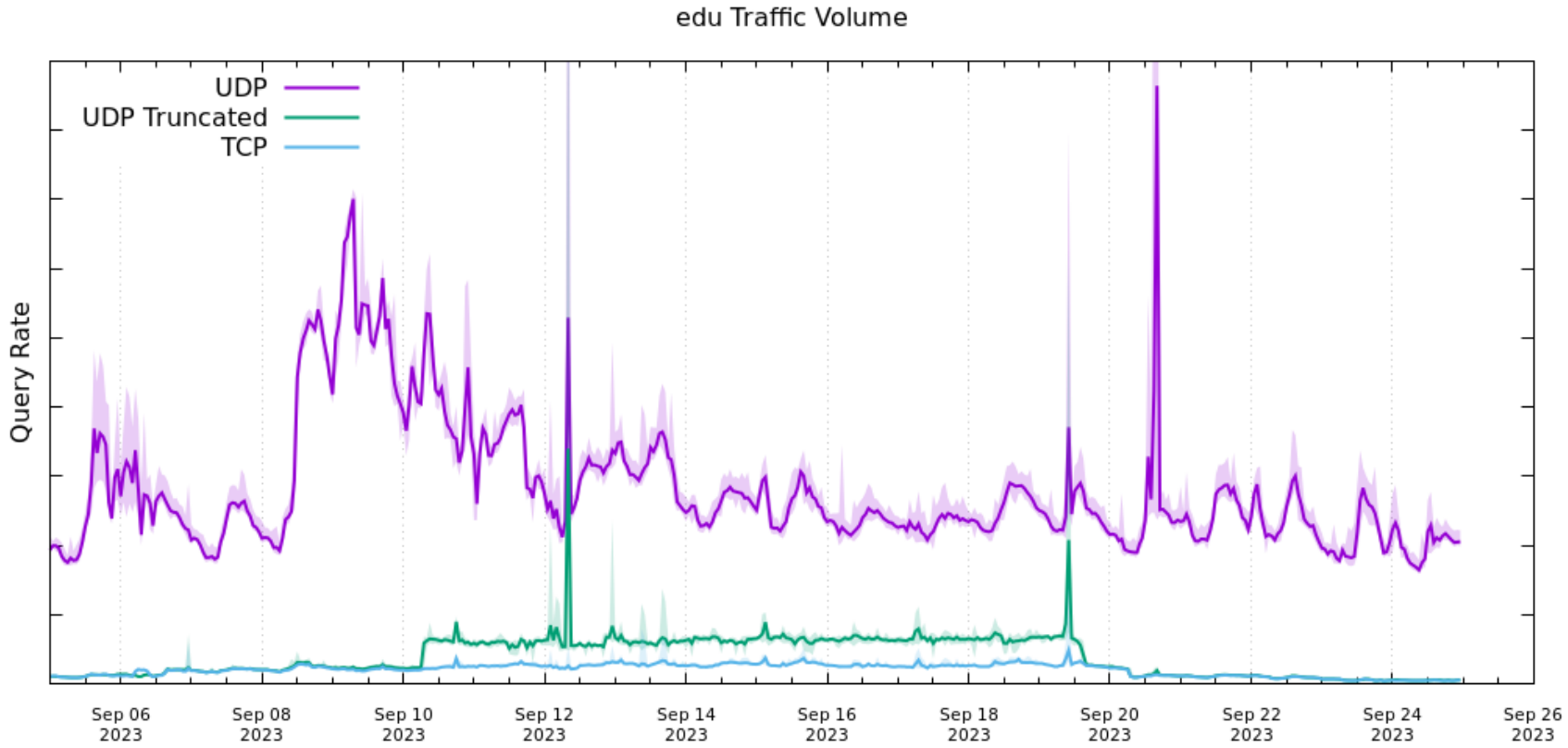
- Due to resolvers unable to query over TCP
- Solutions:
  - Communicate to community
  - Coordinate with large resolver operators
  - Real-time monitoring
  - Outreach if necessary
  - Tweak truncation policy if necessary

Double Signing Algorithm Rollover Schedule

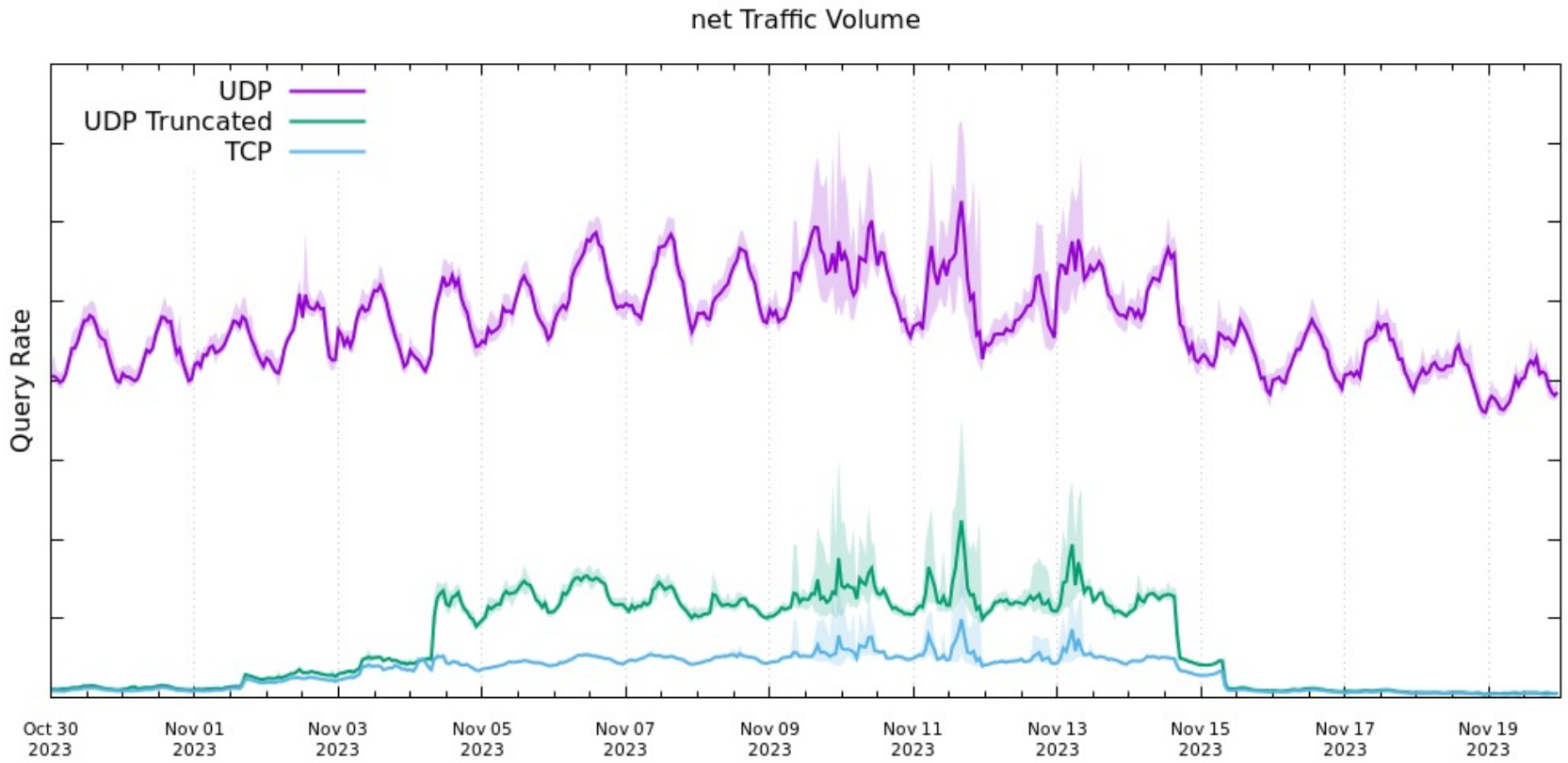
Day	Activity
1	ECDSA keys activated
2-5	ECDSA signatures added
6	ECDSA keys published
7-12	Root zone DS record changed
13	RSA keys un-published
14	RSA keys deactivated
15-18	RSA signatures removed

Traffic Volumes

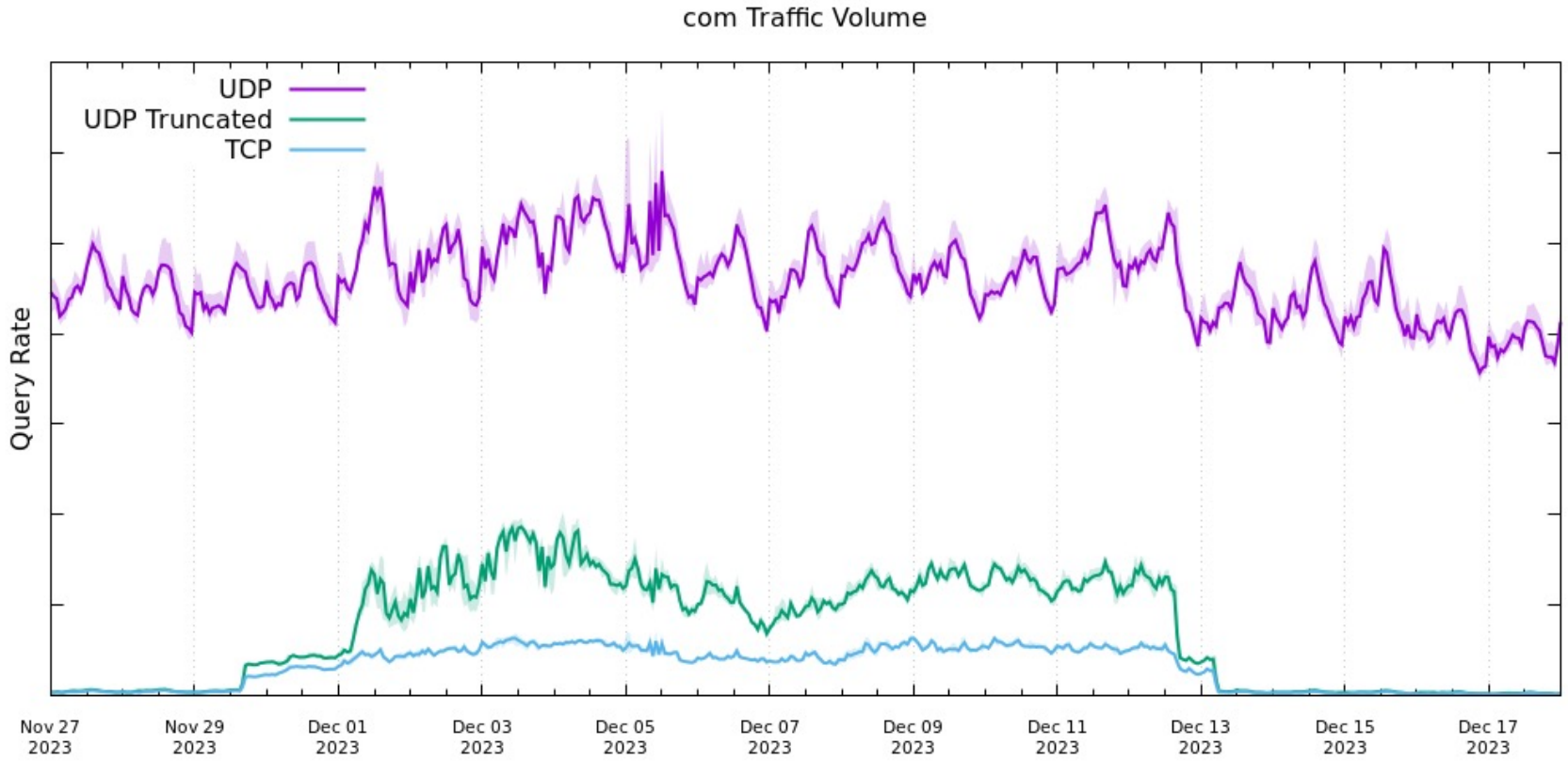
EDU: Sep 6 – 23, 2023



NET: Nov 1 – 18, 2023



COM: Nov 29 – Dec 16, 2023



Response Sizes, Truncation, and TCP

Factors Affecting Truncation

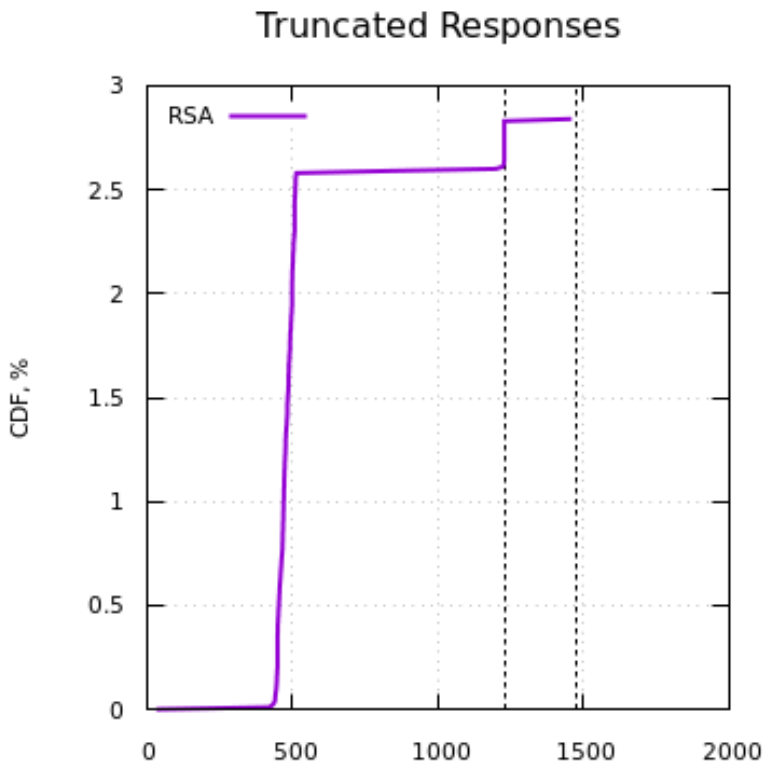
- Client's maximum UDP size
- Server's maximum UDP size
- Number of NS, DS, and glue records
- Glue truncation policy
  - RFC 9471 "DNS Glue Requirements in Referral Responses"

Response Characteristics

Type	Response Size	Signature Count	Risk of Truncation Due to Double Signing
DO=0	varies	0	none
Secure Referral	small	1	minimal
Insecure Referral	medium	2	small
DS denial-of-existence	medium, but fixed	3	minimal
NXDomain	large	4	high

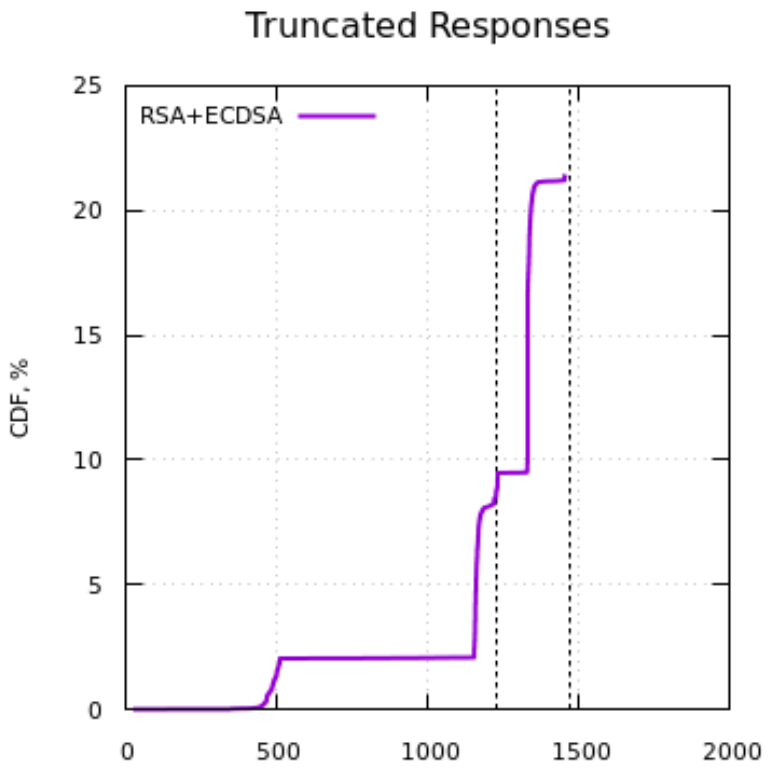
Truncation – Before Rollover

- Before the rollover, most UDP truncation happens around the 512-byte boundary
- A small amount around 1232



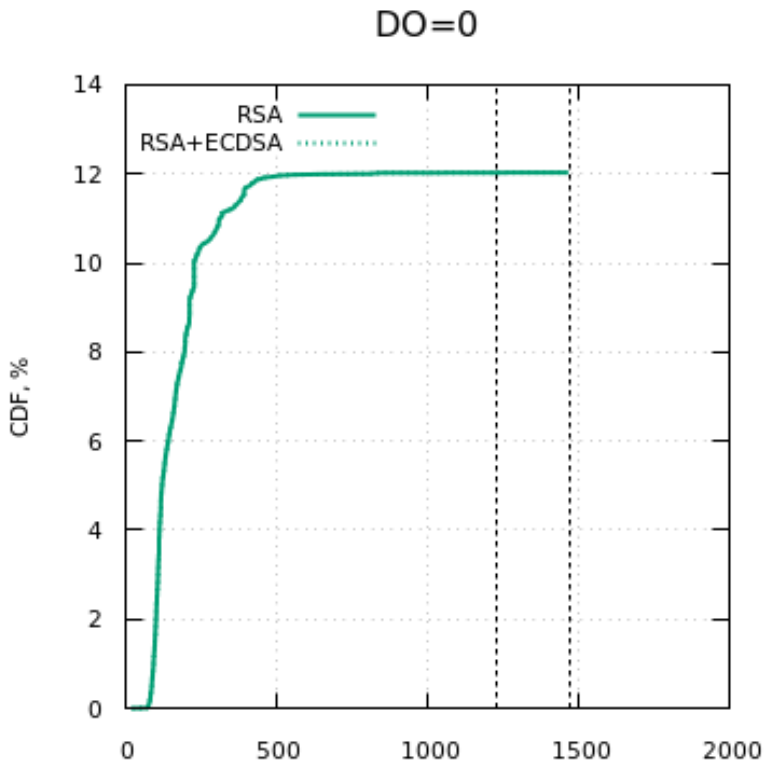
Truncation – During Rollover

- During the rollover, there is a significant increase in UDP truncation (3% – 22%)
- Still some at 512
- More at 1232
- Even more around 1400



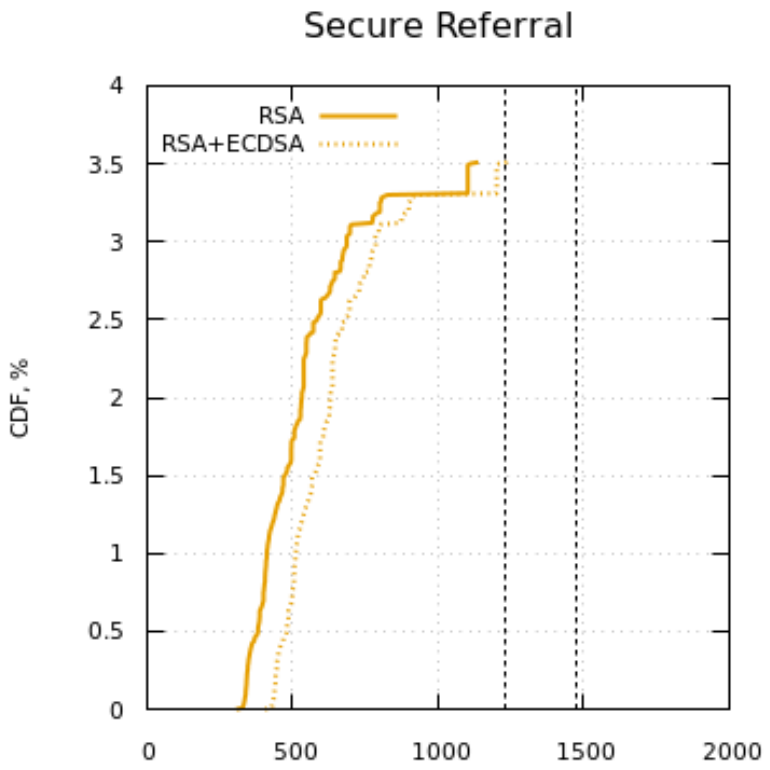
DO=0 Response Sizes

- Pre-rollover 12% of queries have DO=0
- Algorithm rollover would not change the size of these responses



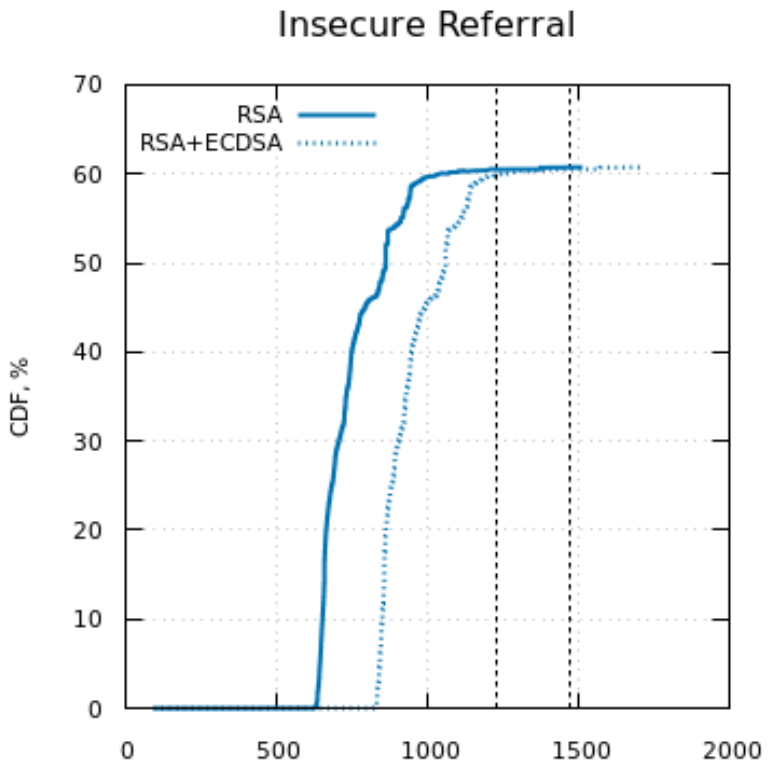
Secure Referral Response Sizes

- Secure referrals have one signature
- Slight size increase during rollover, but still below 1232 bytes



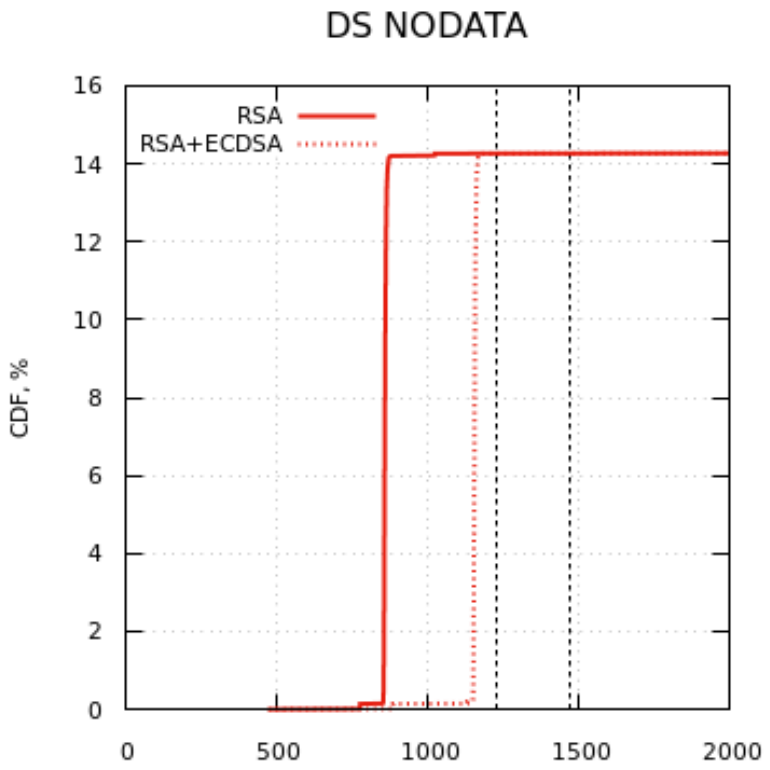
Insecure Referral Response Sizes

- Insecure referrals have two signatures
- Very few responses predicted to exceed 1232
- Most responses (60%) fall into this category



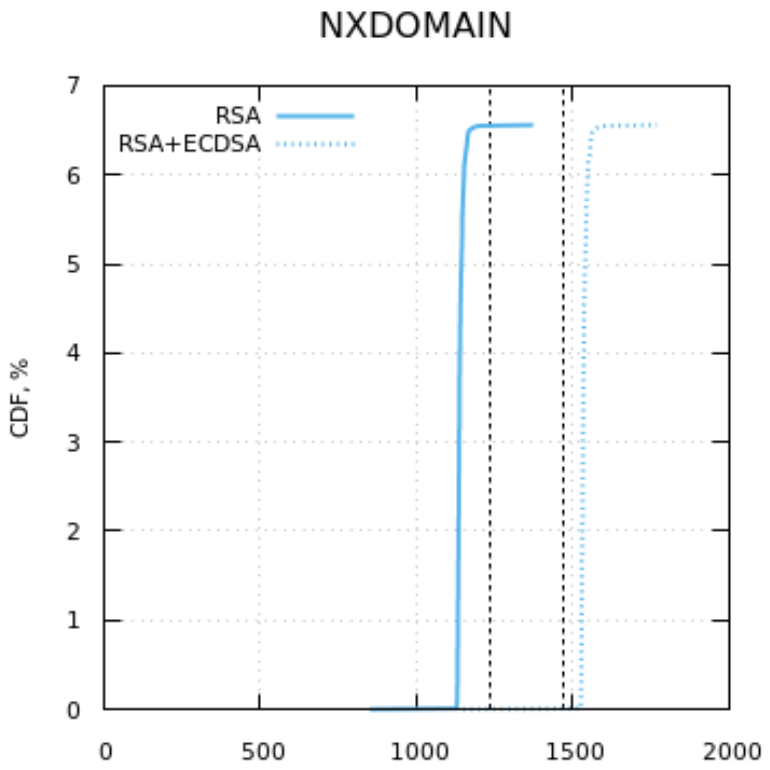
DS NODATA Response Sizes

- DS NODATA responses have three signatures and an almost constant size
- During rollover predicted to stay below 1232 bytes

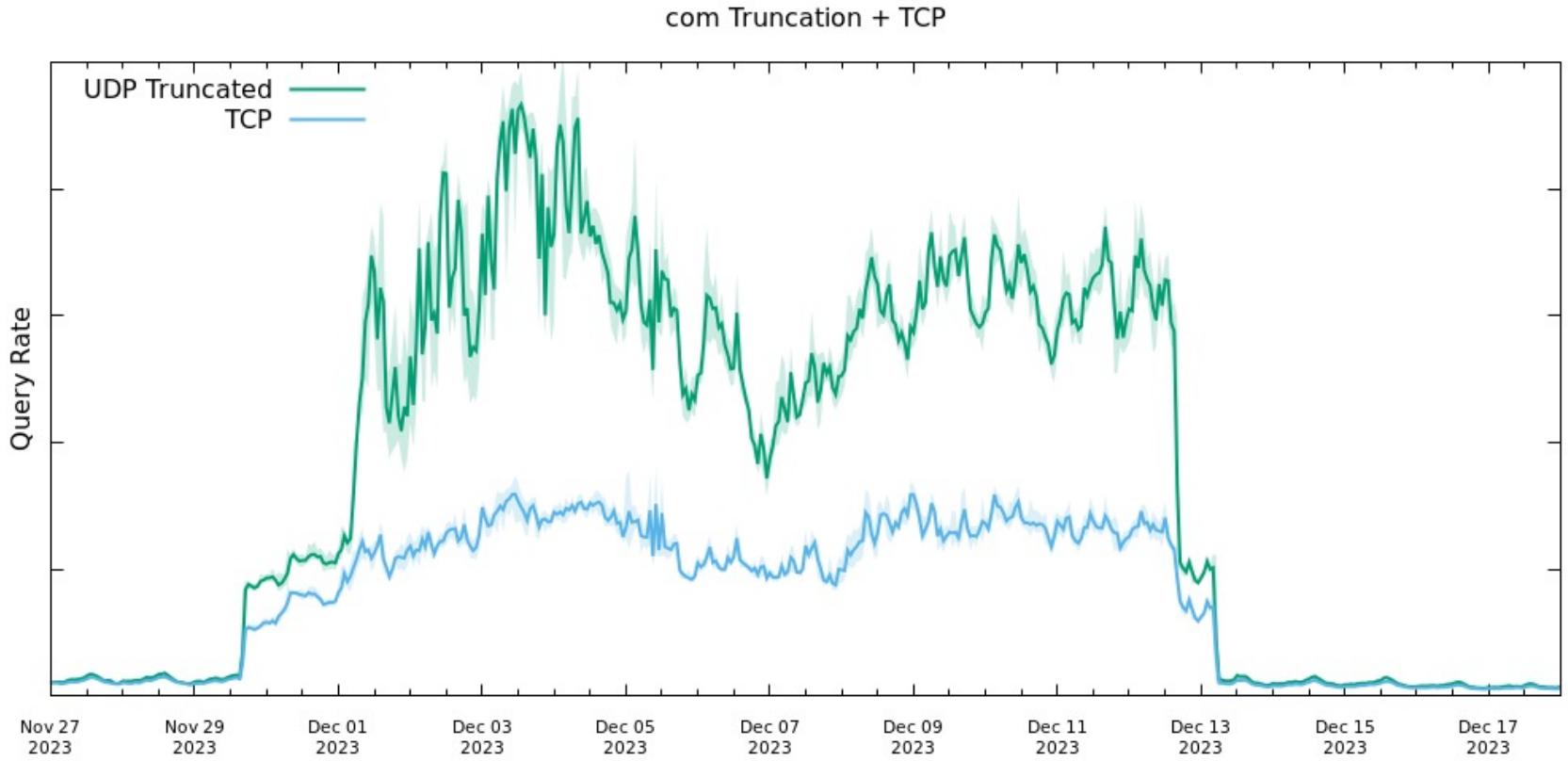


NXDomain Response Sizes

- NXDomain responses have four signatures, and nearly constant size
- All NXDomain responses expected to exceed 1500 bytes during rollover



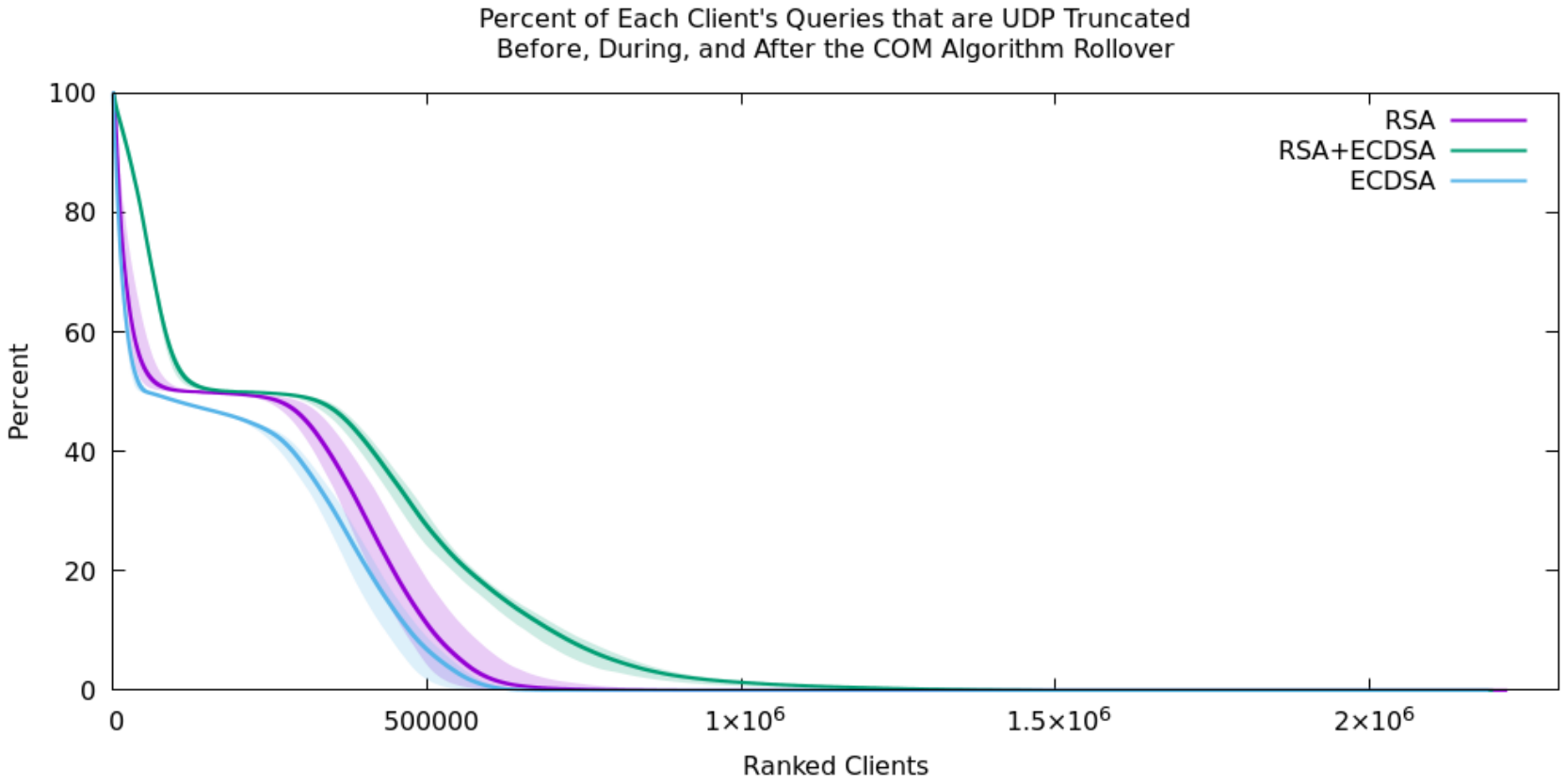
Truncation Levels Higher Than Expected



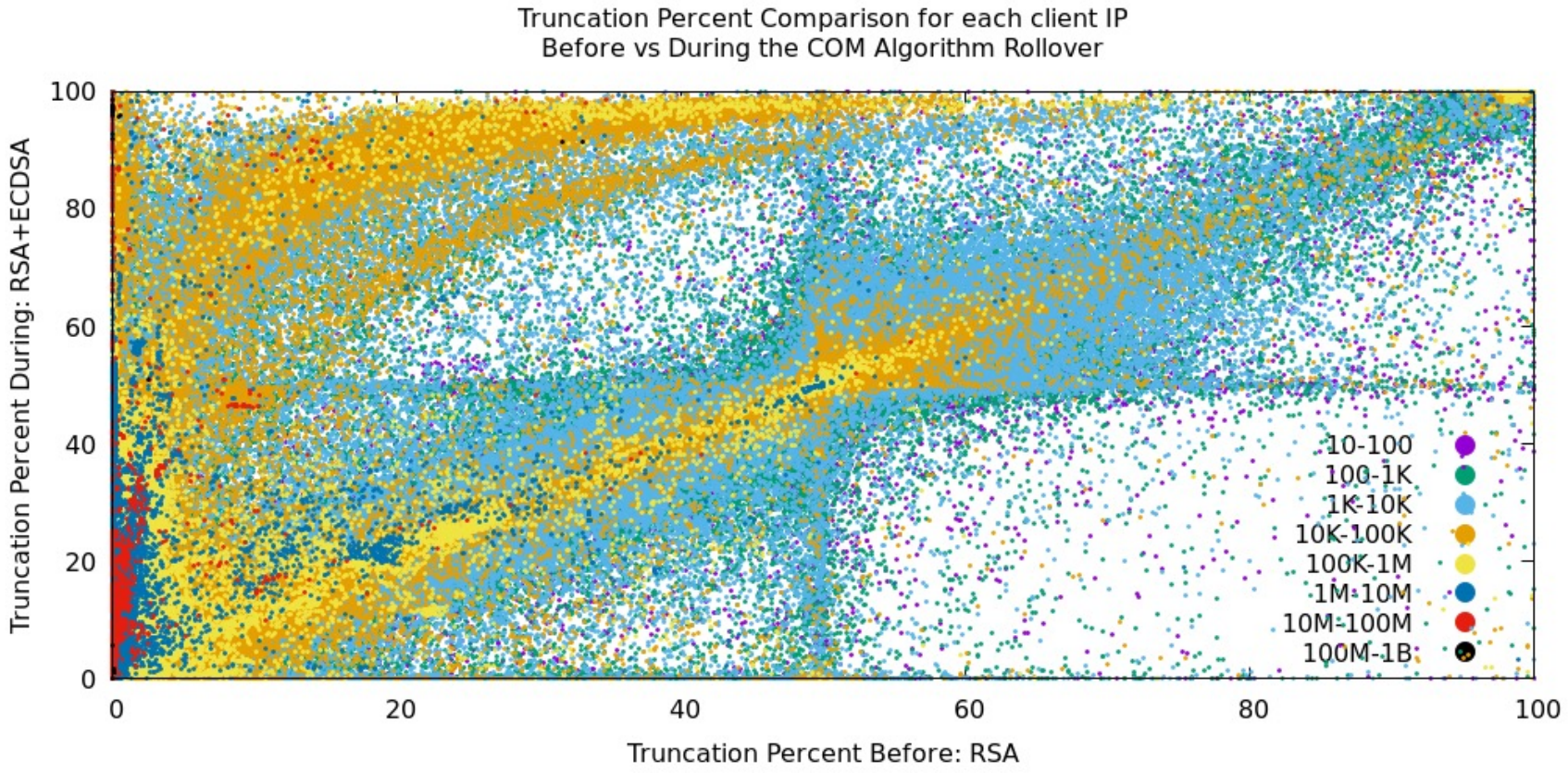
Why So Much Truncation?

- Responses larger during rollover, obviously, but...
- Resolvers unable to query over TCP retry over UDP?
- Non-resolver clients don’t need untruncated response?

Percent of Truncated Responses



Percent of Truncated Responses



Conclusions

- Many resolvers don’t fall back to TCP for truncations
  - No network path for DNS-over-TCP?
  - Not “full service” resolvers?
  - Some aggressive retries over UDP
- Double-signing rollover had minimal impact to resolution of existent domain names
  - Very few popular domain names with large referral responses

VERISIGN®