Finding DNSSEC Validators with Check-Repeat

Duane Wessels

April 19, 2013

VERISIGN

Joint Work

- Yingdi Yu, UCLA
- Duane Wessels, Verisign Labs
- Matt Larson, Verisign Labs
- Lixia Zhang, UCLA

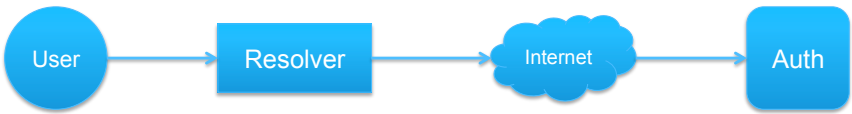
Why Count Validators

- DNSSEC suffers somewhat from the “chicken-and-egg problem.”
- The publication-side of DNSSEC is well studied. The consumer-side, not so much.
- Surveys and estimates of validator population inform the upcoming root KSK rollover (2015).

Enumerating Validating Resolvers is Hard

- Resolver chaining
- Multiple resolvers per user
- Multiple IPs per resolver
- NATs
- Dynamic addressing
- Unexpected query behavior
- Trust Anchor configuration not conveyed in queries

Simplistic Model

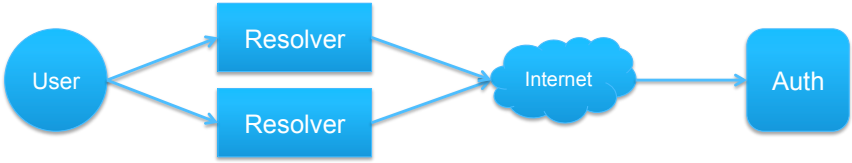


VERISIGN

Chaining

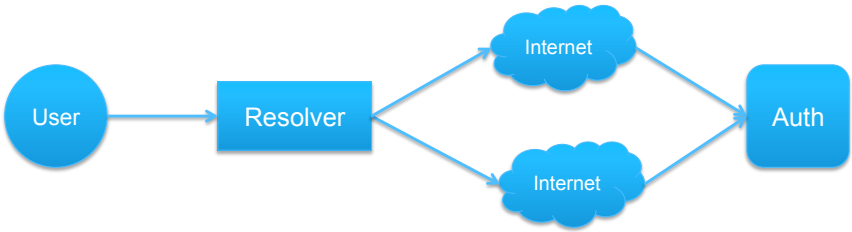
VERISIGN

Multiple Resolvers per User



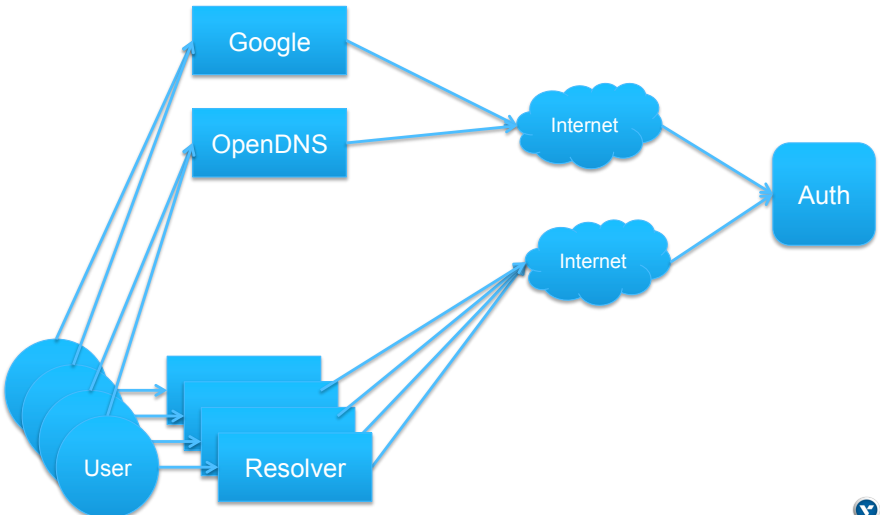
VERISIGN

Multiple IPs per Resolver

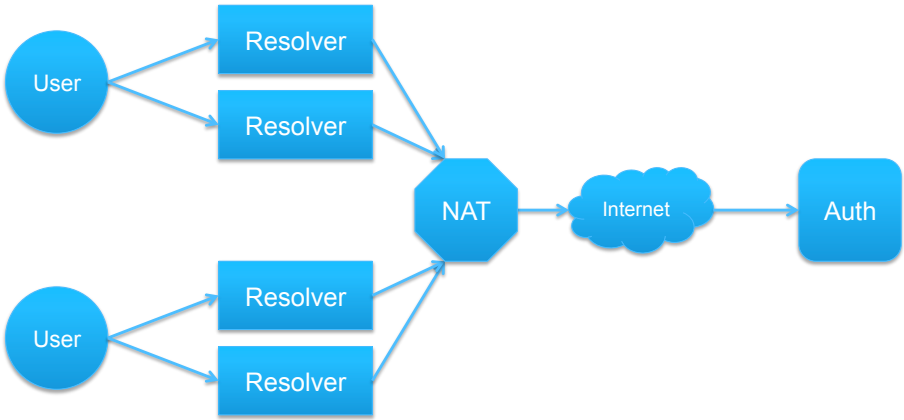


VERISIGN

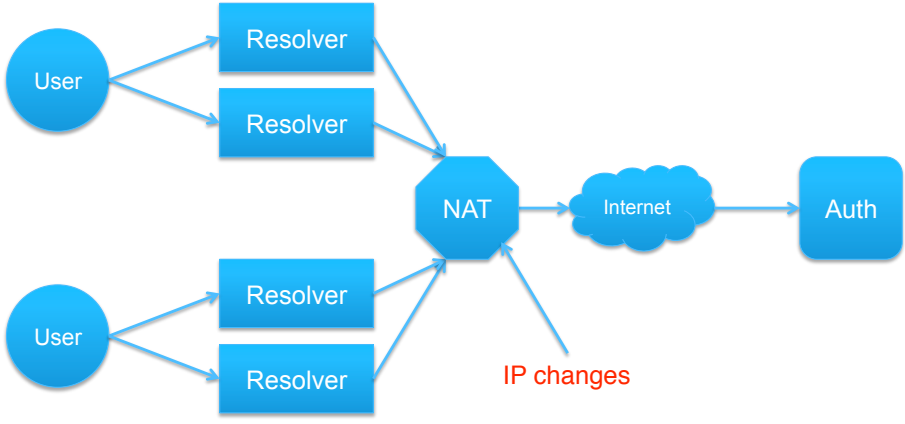
Public Resolvers



NATs

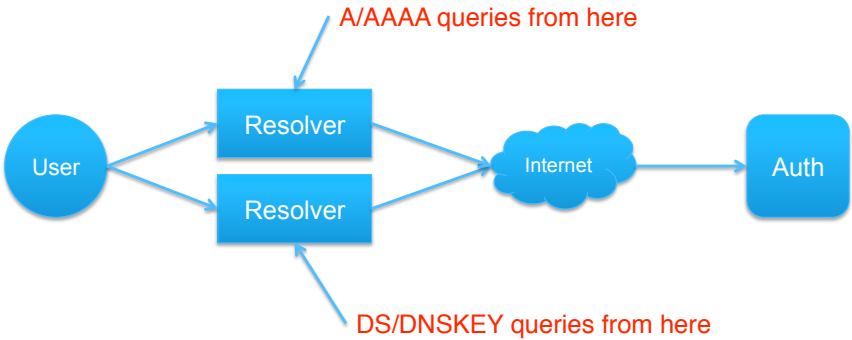

User
Resolver
Resolver
User
Resolver
Resolver
NAT
Internet
Auth

Dynamic Addressing



VERISIGN

Unexpected Query Behavior



VERISIGN

Previous Approaches

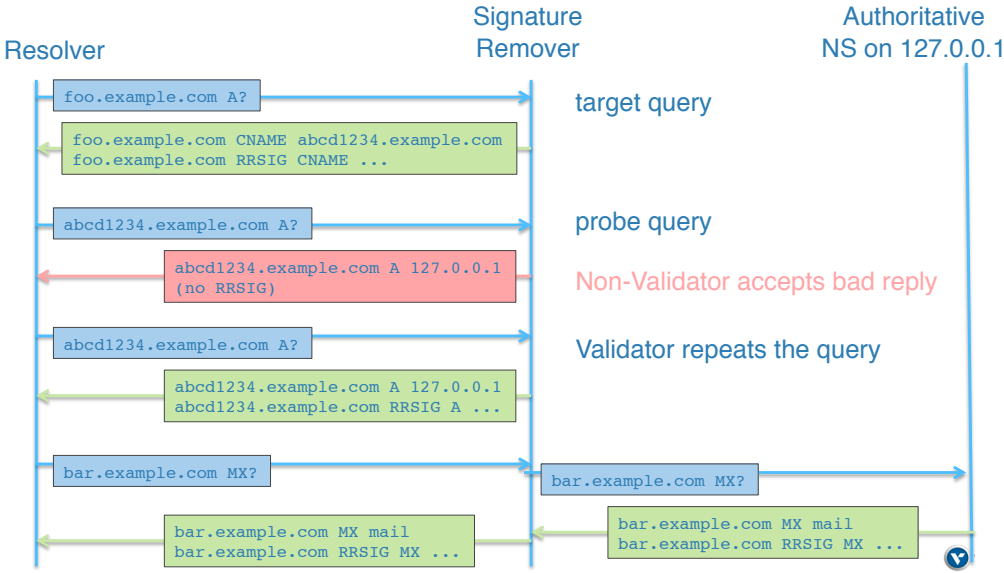
- Look for DNSKEY and DS queries at authoritative name servers.
  - Assumption that only validating resolvers make DNSKEY/DS queries might not be true.
- Correlate DNS/HTTP requests for pairs of DNS names. Lack of use of improperly signed name implies validation.
  - Web browser bias?
  - Good for measuring end user adoption
  - Could measure application-based validation, vs resolver-based.

Check-Repeat

- When presented with an improperly signed DNSSEC response, most validating resolver implementations will retry the query.
  - At least once.
  - To another authoritative name server.

- However…
  - Query retries look a lot like packet loss.
  - Not all implementations retry.
  - Doesn't work for "chained" resolvers.

Signature Remover



How to attract DNS queries?

- A web bug via DNS prefetching.

```
<link rel="prefetch" href="http://prefetch.validatorsearch.verisignlabs.com" />

<a href="http://prefetch.validatorsearch.verisignlabs.com"></a>
```

- Take advantage of popular, yet non-critical domains.

wpad.{com,net,org,us,biz}

- “Web Proxy Auto Discovery”
- Work by Microsoft and others, documented as Internet-Draft but never RFC.
- HTTP agents (browsers) try to load URLs by prepending “wpad” to their local domain:

  `http://wpad.cs.ucla.edu/wpad.dat`
- On failure, try again by removing domain labels:

  `http://wpad.ucla.edu/wpad.dat`

  `http://wpad.edu/wpad.dat` ?

  `http://wpad/wpad.dat` ?

Results

Indicators of Validation

- DS/DNSKEY queries
- Repeats
- Consistent pattern over time

Nominum/Vantio

- Nominum's resolver product, Vantio, does not consistently retry signature-removed queries.
- Fortunately, Vantio openly answers "version.bind" queries by default.
- Whitelisted for this study.

Trace-I

Totals	
Days	36
Queries	24,786,845
Trials	6,498,277

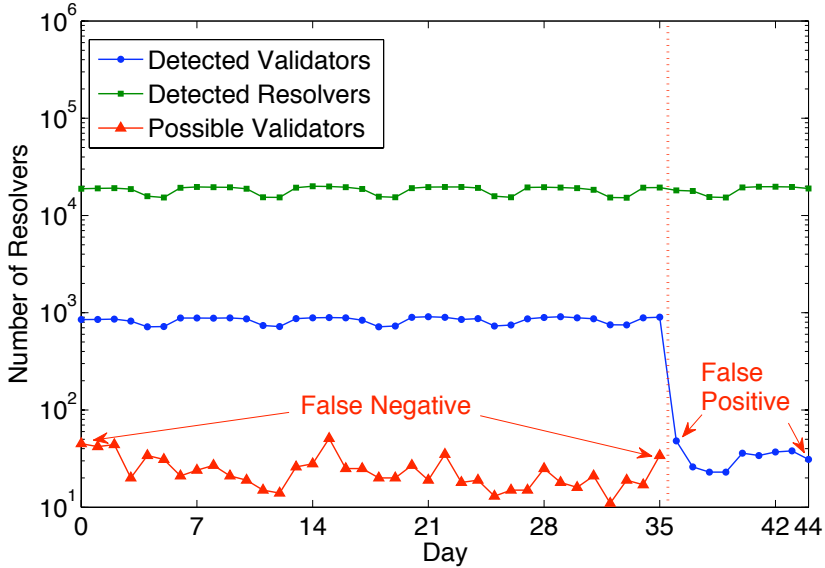
Daily Averages	
IPs	24,143
Resolvers	18,224
Validators	836
%Validating	4.6%

Quantifying False Positives

- Queries repeated due to packet loss could be misinterpreted as validations.
- Signature remover disabled for 9 days to find false positives.

Daily Averages	
IPs	24,522
Resolvers	18,247
Validators	33
False Positives	0.18%

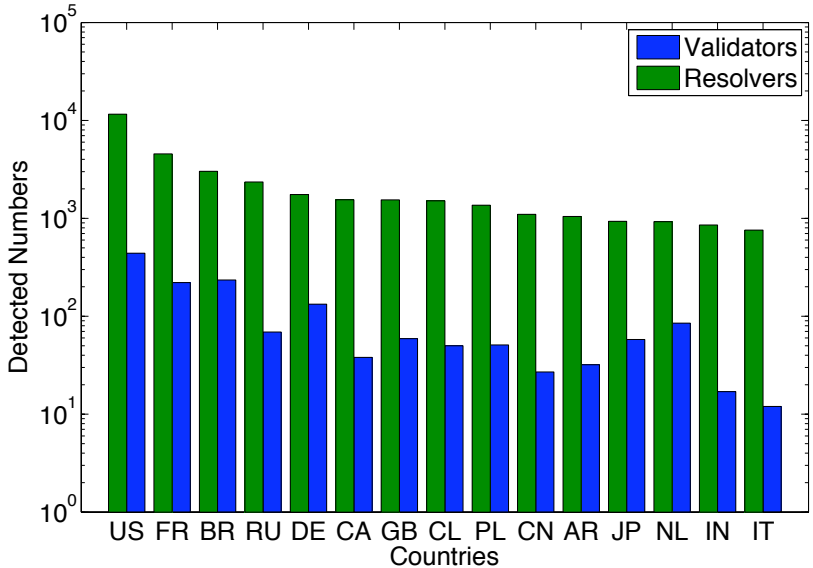
Number of Resolvers and Validators Measured



Quantifying False Negatives

- Cases where resolver received DNSKEYs, signatures were removed, but did not see repeated query.
- Likely caused by multi-level caching, a.k.a. DNS forwarding.
- About 30 false negatives out of 20,000 resolvers daily.
- False negative rate 0.15%.

Geographic Distribution of Validating Resolvers



Did we find all Resolvers on the Internet?

- Compared resolvers observed by Check-Repeat to those seen by G.GTLD-SERVERS.NET (one of 13 COM/NET name servers).
- Check-Repeat sees 1.6% of resolvers seen by G.GTLD.
- But 63.5% of all responses from G.GTLD go to Check-Repeat resolvers.
- At least 12.3% of all responses from G.GTLD go to DNSSEC validators.

Comparison with Previous Work

- [2010] Gudmundsson and Crocker found 10% (upper limit) of queries to ORG name servers are from resolvers that ask for DNSKEY/DS.
  - We find 12.3% for COM/NET (lower limit)
- [2012] Wander and Weis report 4.8% of *trials* indicate validation.
- [2012] Huston reports 9% of Internet *end users* have validating resolvers and 4% of resolvers validate.
  - 7 days of data
- [2012] Huston later revises and reports 1.6% of *end users* and 1.7% of *resolvers* perform validation.
  - 17 days of data
  - We find 4.6% (of resolvers)

Thank You

VERISIGN