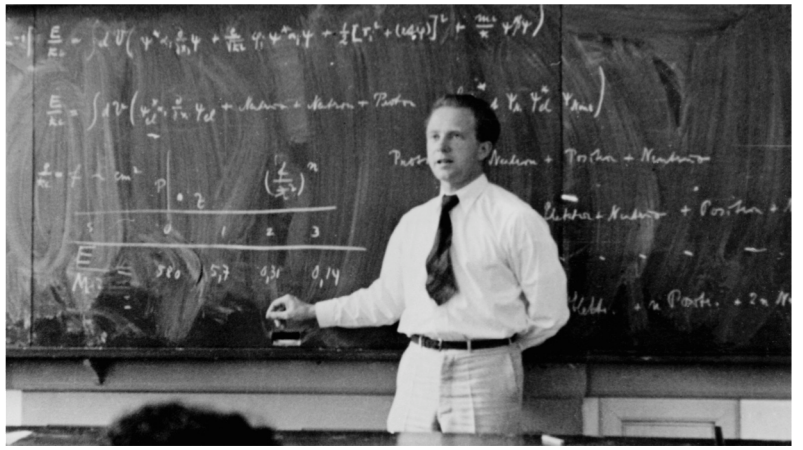
Heisenberg’s DNS

Werner Heisenberg



1901 – 1976, German Theoretical Physicist

Uncertainty Principle, published in 1927:

$$\sigma_x \sigma_p \geq \frac{\hbar}{2}$$

There is a fundamental limit to the precision of the simultaneous determination of a particle's position and momentum

Heisenberg’s Principle applied to the DNS

There is a practical limit to the precision that can be used when measuring the resolution behaviour of the DNS

Why think about this?

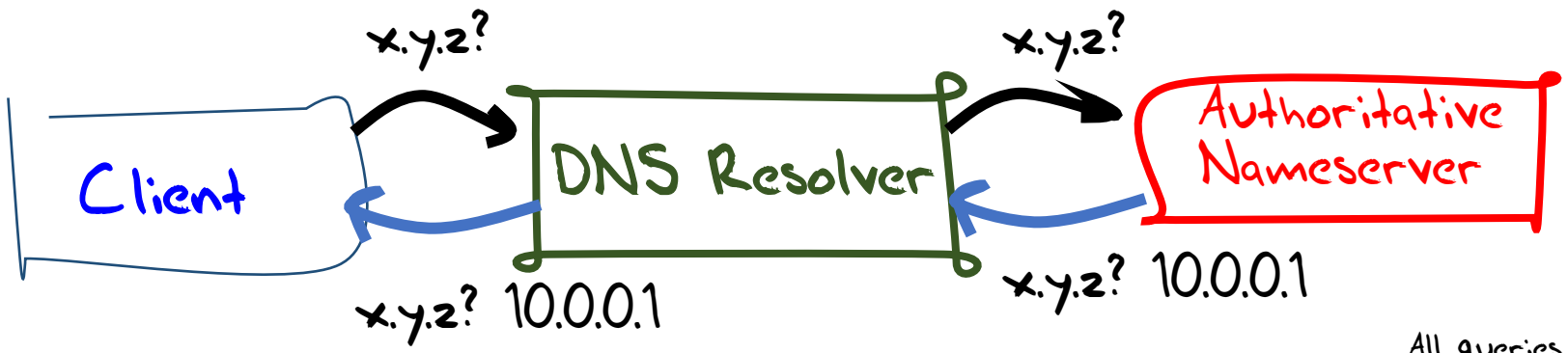
Because we are using DNS measurements in many of our reports and studies:

- DNSSEC deployment
- KSK roll
- NCAP

- In these reports we appear to be assuming that we understand the concepts of precision and uncertainty when applied to the DNS
- And we may be giving the impression that we are capable of quantifying the uncertainty associated with any measurements that we may use or cite
- This is probably not the case!

Models of DNS Name resolution

A simple-minded view of DNS resolution



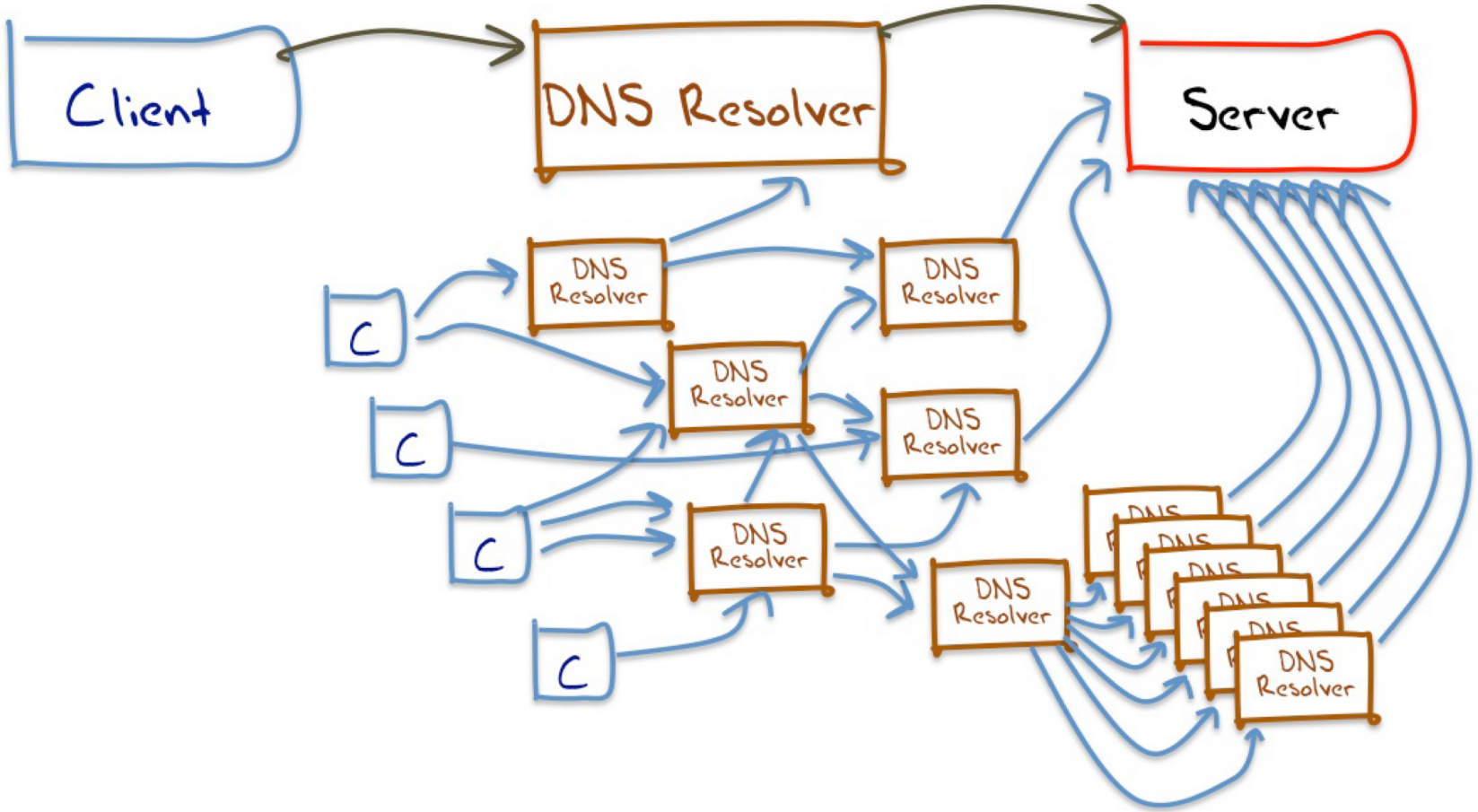
Each resolver may have many clients

All queries received by the resolver are passed to authoritative servers, together with the resolver's own name server discovery queries

Models of DNS Resolution

- On the resolver side:
  - Add in caching, load balancers and resolver farms, slave query agents, forwarder lists, policy directives, aggressive NSEC caching, use stale
- On the client side
  - Client-side resolver lists, re-query and abandon timers
- On the server side
  - Anycast server constellations

A Larger View of DNS Resolution

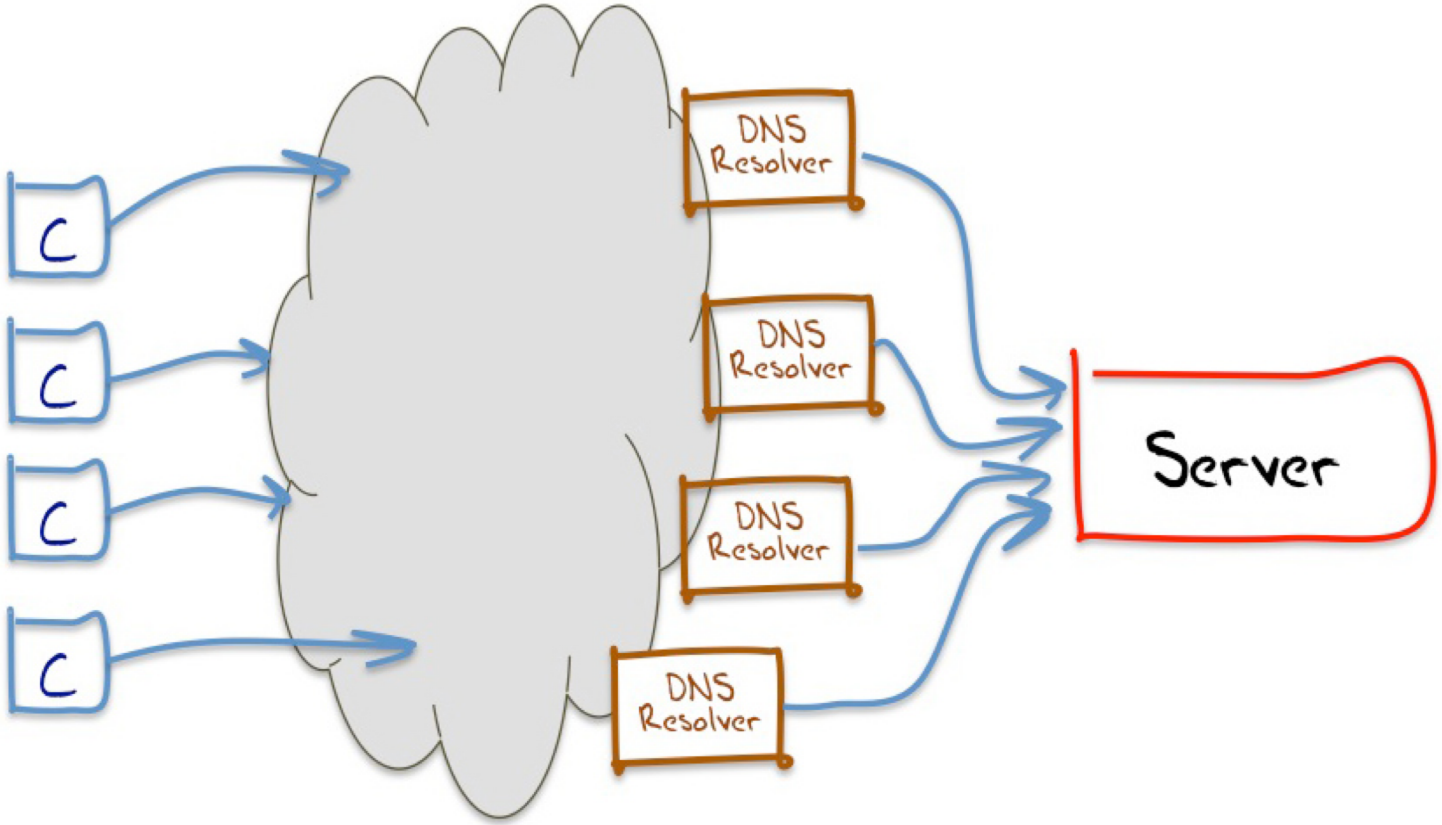


A small sample of what appears to happen in DNS resolution

DNS as a Cloud Service

The interior of the DNS resolution environment is largely opaque from external view

DNS queries have no explicit tracking capability, and the internal structure of resolvers, forwarders, load balancers and intercepting middleware is challenging to expose to external observers



The best model we can use for DNS resolution

How can we measure the DNS?

There are two major forms of approach to DNS measurement:

- **Passive measurement** entails collecting logs of queries at authoritative servers or at recursive resolvers and inferring behaviours of the DNS from analysis of these logs
- **Active measurement** entails generating client-side queries and observing the responses from the DNS system

Passive Measurement

Root Server Query Data

- Day in the Life (DITL) is one of the few public access points to root server query data
- Root Servers are meant to serve root zone priming queries and recursive resolver Name Server discovery local cache miss queries
  - They appear to see much more than this – why?
- They are meant to serve the contents of the root zone, yet the majority of their queries concern domain names that do not exist
  - Most queries (~70%) to root servers generate an NXDOMAIN response from the root server
  - Most queries (~95%?) to root servers ultimately generate an NXDOMAIN response from a server
- DNS Privacy measures are eroding the utility of these measurements
  - Adoption of Qname minimisation in recursive resolvers
  - Adoption of DNSSEC-signed zones coupled with the adoption of Aggressive Use of NSEC caching by security-aware recursive resolvers

Passive Measurement

Authoritative Servers

- Very little published data
- Lack of consistently published data sets of queries from authoritative servers
- Probably have the same limitations / issues as root servers

Recursive Resolvers

- Very little in the way of published data
- The context of a recursive resolver probably has a distinct bearing on the queries that are passed to the resolver

Active Measurement

- Inject queries into the DNS
  - Used in One-to-Many experiments
    - E.g. DNS queries to the Alexa top 1M names
  - Relatively easy to instrument on the client side, but hard to control exactly how the DNS behaves in response to the query
  - Used in Many-to-One experiments
    - APNIC AD-based measurement system
    - Relatively easy to inject a query, but relies on an instrumented server
    - Challenging to determine if the client receives the DNS response
    - Question over the potential bias in selection of clients

Some DNS questions

- What is the extent of DNS interception?
  - We know it exists, but we don't understand how to quantify it
  - How can we measure it?
- Why is the NXDOMAIN response rate so high for root servers?
  - How can we test an hypothesis as to why this is happening?
  - What would be the reliability of any such test?
- Do root servers see a different profile of queriers than other authoritative servers?
- What's the query repeat rate (zombie queries) for the DNS?

Recent / Current SSAC Issues

- KSK roll
  - 2018 planned roll
  - KSK roll to new algorithm
  - KSK emergency key roll procedures
  - KSK synch mechanism
  - What's "safe"? How can we measure "safe"? What is the quality of such a measurement?
- NCAP Study
  - What's a "collision"?
  - How can we measure the incidence of collisions?
  - Can we quantify the consequence of collisions?

Discussion Points

- Who is measuring?
- What data sets are they using?
- What should we be measuring in the DNS?