RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Measuring DNS without breaking anything

RIPE Atlas

Christopher Amin | 2019-05-20 | RIPE 78

RIPE Atlas safety

- Measurements can be scheduled from any probe(s) to any target
- Probe hosts should not get in trouble due to measurements on their probes
- Probes should not be able to cause harm to (sensibly configured) targets
- We will always act responsively to fix abuse that comes up (stop measurements, ban users)

DNS Measurements

- DNS lookups using locally available recursive resolvers or a specified name server
- No restriction on which servers can be queried, although there are rate limits per target
- DNS over TLS (DoT) supported

HTTP(s) Measurements

- Fetch a single HTTP(s) resource and record statistics
- Concern that asking probes to request a resource that is forbidden in its location could compromise the host
- Whitelist of targets (RIPE Atlas Anchors) that should be “safe”
- Trusted users can bypass the whitelist with our agreement

Bringing them together: DNS over HTTPS

- Not currently supported by RIPE Atlas
- Not easy to tell apart from other HTTPS queries
- Whitelist of targets would make it much less useful
- Just getting TLS cert from arbitrary host (on e.g. 443) is supported already, but no complete handshake

EDNS Options

- Subset of EDNS options codes (and flag) supported
- Not all documented codes are supported. What should we add? Flag Day
- Currently undefined values are not supported at all
- Makes it difficult to test new/ experimental DNS features using RIPE Atlas

`udp_payload_size`

`cookies`

`set_nsid_bit`

`set_do_bit`

`default_client_subnet`

(0/0 and ::/0 only)

So…

- Should RIPE Atlas support DNS over HTTPS?
  - How do we make it “safe” for probe hosts?
  - Could the same be applied to HTTP(s) measurements?
- Should RIPE Atlas support (currently) undefined EDNS options?
  - Could that be abused? In theory undefined options should be ignored…
  - Could we keep it relatively “safe” for DNS servers?
- Mailing list: ripe-atlas@ripe.net
- Me: camin@ripe.net
- Questions?