IP Address Privacy

Interim Summary

Agenda

- IP address use cases
  - Anti-fraud and abuse: Dimitris Theodorakis (WhiteOps), Philipp Pfeiffenberger (YouTube), David Turner (Google) (20 mins)
  - DDoS: Damian Menscher (Google) (10 mins)
- Privacy implications of IP Addresses:
  - Overview of privacy implications: Fernando Gont (SI6 Networks) (15 mins)
  - Server-side address privacy: Christian Huitema - TBC (Private Octopus) (15 mins)
- Techniques for hiding IP addresses
  - Anonymity networks and tokens: George Kadianakis (Tor) (15 mins)
  - Using Multicast DNS to protect privacy when exposing ICE candidates (https://datatracker.ietf.org/doc/draft-ietf-mmusic-mdns-ice-candidates/), Justin Uberti (Google) (15 mins)
  - Willful IP Blindness: Brad Lassey (Google) (15 mins)

Key Questions

If IP addresses were removed, what sort of signal would be needed to protect anti-abuse use cases?

What are the privacy costs and service benefits for using IP addresses as signals?

How do IPv4 and IPv6 addresses affect signal entropy?

Is (unspoofable) remote attestation enough for a signal? If not, can anonymous credentials be used instead?

Next Steps

Document client and server requirements for a suitable signal replacement

- Clients want privacy (and more), servers want utility

Consider how this can be built with standard technologies

- TLS ECH, MASQUE, Oblivious HTTP/DoH, Privacy Pass

Consider impact of technologies on the ecosystem

- Proxy selection and trust? Centralization?

Decide where to do this work

- PEARG? Elsewhere?