Privacy Enhancements and Assessments Research Group Agenda - IETF 110

Administrivia (5 minutes)

- Blue sheets / scribe selection / NOTE WELL
- Agenda revision

New Work / Presentations (45 mins)

IP Address Privacy (continued from the Interim….)

Techniques for hiding IP addresses

- Gnatcatcher: Brad Lassey, Paul Jenson (Google) (15 mins)
- From privacy sandbox team
- First step third party cookies
- Need to ensure not allowing other linkage IP big one
- Many addresses per person/many person per address/not use for identity
- Only IPv6, SLAAC keeps prefix same, randomized routing slow
- Gnatcatcher is combination of NAT and IP address blindness
- Willful blindness: servers attest they don't, audits to determine truth
- Then given certificate for browser to adjust privacy budget
- Can split into two halves, one with IP address one with application data. CDN could offer as a service
- Server selection based on IP: tricky, involves GeoIP
- Need to fall back to auditing
- Anti absue uses IP: will have to carve up applications and separate across the stack
- CDN application split achieves this sepaation
- Trust tokens to decrease application reliance
- IP to region for region-specific treatment (CCPA, GPDR)
- Audit will need to look at this
- Debugging performance, investigating dangerous abuse
- 27 bits out of 33 bits
- IP eats up privacy budget!
- Cross-site abuse mechanisms need audits to keep working

- Near Path NAT: IP Privatizing Server
- Run at CDN level
- Prevents tracking across sites including reidentification
- HTTP/3 to nat, proxy things through
- By being on the edge performance is not decreased
- Avoids going far off path
- GeoIP: geographic location preserved since these are near clients
- IP port tuple per client and top level site preserved
- Trust tokens can help
- Facilitiates within site antiabuse
- MASQUE is providing exactly what is needed
- Mark Nottingham: a few slides at "edge."" Many different things to many people. Where and run by who?
- Paul: Just a proposal. At CDN one answer. Who runs it: don't know of great answer. doesn't need to be one person.
- Mark: Need mechanism to have virtuous cycle
-

- Presented by Chris Wood
- Entire focus of interim on IP privacy
- How used? Anti abuse, DDoS mitigation
- Privacy implications
- Hiding proposals: Tor, ICE, Gnatcatcher/IP blindness
- Key Qs:
- Anti-abuse without IP
- IP as signal costs
- IPv4 and IPv6 signal entropy
- remote attestation? anonymous credential
- Need to get clarity on requirements from all parties. Would work on a replacement
- Next steps: document requirements, consider existing technologies, impact on ecosystem, decide where to do this work

- Bradford Lassey: Having a forum for discussing needs and how applications could affect them would be great.
- Stephen: PEARG a good venue to include scope about IMC and mobile. In IETF would soly focus on IP address mechanism.
- Chris: don't want to over constrain ourselves
- Matthew Finkel: Work won't result in single drop in replacement. Different solutions for different signals.
- Chris: Geo, identity, all different. Different mechanisms likeley
- Andrew Campling: network operators, ent and public, make sure stuff isn't broken. Downsides of making things more private
- Chris: specifically want people in conversation who are using this and understand why and how and work as a group on suitable set of replacements if needed.
- Stephen: One issue is how IP addresses used as headers in mail. Similar anti abuse. Should this be in scope or really just web?
- Chris: good question. I don't know, curious about others. Web matters.
- Stephen: a bit different.
- Stephen: M3AAWG is group that knows. Reluctant to change
- Sara: Might group things together, fall out is signals with different nature.
- Chris: part of requirements generation.
- Shivan: Are people interested in writing this draft
- Joey: MARDINAS BOF meeting 109 and 110, cases broken with MAC randomization are now consolidating solutions in a couple of drafts. Use cases in mind right now for IPs.

Routing for Anonymous Communications - Zach Newman (15 mins)

- Early stage research joint with a number of people
- Overlay routing benefit decentralized systems
- Case study Tor
- One real world deployed system: Tor!
- Application goals: security and privacy cannot be impacted
- Some preliminary evidence in favor. Will build out further and should get more info
- UNDER CONSTRUCTION! AUTHORS AT WORK!
- CDNs go faster with overlay: go through intermediaries that can avoid slower paths. Internet routing is not best latency

- Machines everywhere, need to be proxies.
- Global view of network conditions.
- Tor can do the same: everywhere, is a proxy!
- Traffic between pairs of relays already there
- Overlay routing influences path selection: additional hops in the same sequence of relays
- Via node doesn't decrypt
- Lots of orthogonal modification proposals, not adding encryption hops.
- Data: analysis of latency between nodes
- more than 100ms speedups sometimes
- FIN->US via hop in europe easier
- Some really terrible default routes
- Scale up latency measurements
- Is this secure? how is anonymity impacted
- Would it work in practice or bring network down
- Wes: middle nodes making decision about how to route. Could they do it pessimally
- David: How to avoid overloading?
- Kyle and Zach: nodes would race
- Watson: client side
- Zach and Kyle: Hard to coordinate, not real time
- Russ: Similar to fibbing (fibbing.net) ## RG draft updates (10 minutes)

A Survey of Worldwide Censorship Techniques, Stan Adams (10 mins)

- Am lawyer, bit out of depth
- Draft authored primarily by Joe Hall
- Techniques used by network operators around wold to block things at bhenst of the state
- Up to date, constant evolving, someone needs to update to keep it living document
- Basically unsustainable
- Consensus to bring to close, date it, ship it
- Almost there
- Minor terminology debate, a few references, bigger issues on relationship between things.
- None seem like that big an issue
- Needs help to resolve
- (https://github.com/IRTF-PEARG/rfc-censorship-tech/issues)
- Volunteers needed!
- Please don't add more issues :P
- Hope to spend some time in next three or four weeks to finish
- Collin: Snapshot?

- Shivan: yes, should last call soon