# Multicast Security and Privacy Considerations

draft-krose-multicast-security

Kyle Rose
Jake Holland (presenting)

# Problem: scalable delivery

- ISP Access congestion => performance degradation
  - Major gap between peak demand and capacity (for >12-15 events/year)
- Capital costs ~= peak load
- Peaks driven by popular content
  - Peaks come both from web and non-web traffic
- Getting worse
  - More TV viewers online, OTT providers bidding on major sports delivery
  - Higher resolution smart TVs using web APIs/embedded browser implementations
  - Larger video game/OS downloads

Non-solutions:

- “Application-level multicast” (unicast with deep caches)
- Peer-to-peer

# Multicast to the Browser at IETF

- dozens of informal conversations, IETF 102-105
- mboned report each meeting IETF 106-112
- Hackathons, POC implementations
- adopted drafts:
  - draft-ietf-mboned-dorms
  - draft-ietf-mboned-cbacc
  - draft-ietf-mboned-ambi
  - draft-ietf-mboned-mnat*
- IETF 111 Bar Bof: https://www.youtube.com/watch?v=vKHdTrhQHLo

# Multicast to the Browser, non-IETF

- Outreach
  - Over 30 ISP conversations, over 30 content owner conversations
  - NANOG, APNIC, Podcasts
  - 5 lab trials with ISPs and co-geo content owners
    - Auto-Ingest with AMT (RFC7450) + DRIAD (RFC8777) with CBACC+DORMS
    - ISP's multicast network gear
    - Issues resolved with MNAT
  - ISP Summary
    - looks good, we'll do this if it makes peaks go away (mostly)
  - Content Owner Summary
    - looks good, we'll do this if performance ok, our players still work
- Chromium
  - fork with demo API: https://github.com/GrumpyOldTroll/chromium_fork
  - Multicast Receiver ported to wasm, playing multicast video: https://www.w3.org/2021/10/TPAC/demos/multicast.html
  - intent to experiment feedback:
    **not ready**, needs confidentiality in design, at minimum
- W3C Community group: https://www.w3.org/community/multicast/
  - Phase 1: webtransport
  - Phase 2: fetch, xhr, h5 download, webrtc (w/ server)

# Multicast Security

- Integrity & Authenticity:
  - Separated from Confidentiality
  - Existing (TESLA/signed packets) and new (AMBI/ALTA) solutions
  - Anchored with secure unicast
- Confidentiality
  - many receivers must decode same packets
    - Decryption keys cannot be 1-to-1, regardless of symmetry
  - Privacy considerations key differences(?) with unicast:
    - Bad: exposes new info to local network/next-hop router
    - Bad: contents very discoverable
      - But: multicast mainly applicable to highly discoverable traffic via traffic analysis
    - Good: removes destination IP address, much increasing anonymity North of access
  - Threat model
    - gap in literature? Or only pervasive monitoring and personal information are concerns?
    - Private browsing mode block is sufficient?

# Existing and Likely Future Related Work

- draft-krose-multicast-security
- draft-ietf-mboned-ambi (AMBI)
- TBD: Mandatory-to-implement cipher suite companion to AMBI (as in RFC 7696)
- TBD: At least one QUIC extension
  - Maybe an evolution of draft-pardue-quic-http-mcast
  - Need to signal datagram multicast channel from unicast, possibly via ALT-SVC or a new frame
- TBD: At least one webtransport extension
- TBD: Probably a secure profile of large-file transport (e.g. FLUTE/FCAST)

Blockers:

- Are the security questions fundamentally addressable, or is multicast DOA for modern internet on security grounds?
- Needs some consensus with security expert opinions

# Disposition?

- Suitable for IETF work?
- If so, recommendations?
  a. Reopen msec?
     - With recharter? (“Group Controller”/GDOI pretty sketchy for broadcast…)
  b. BoF for Broadast msec?
  c. Other options?
     - (reopen msec mailing list?  Or make a new one?)