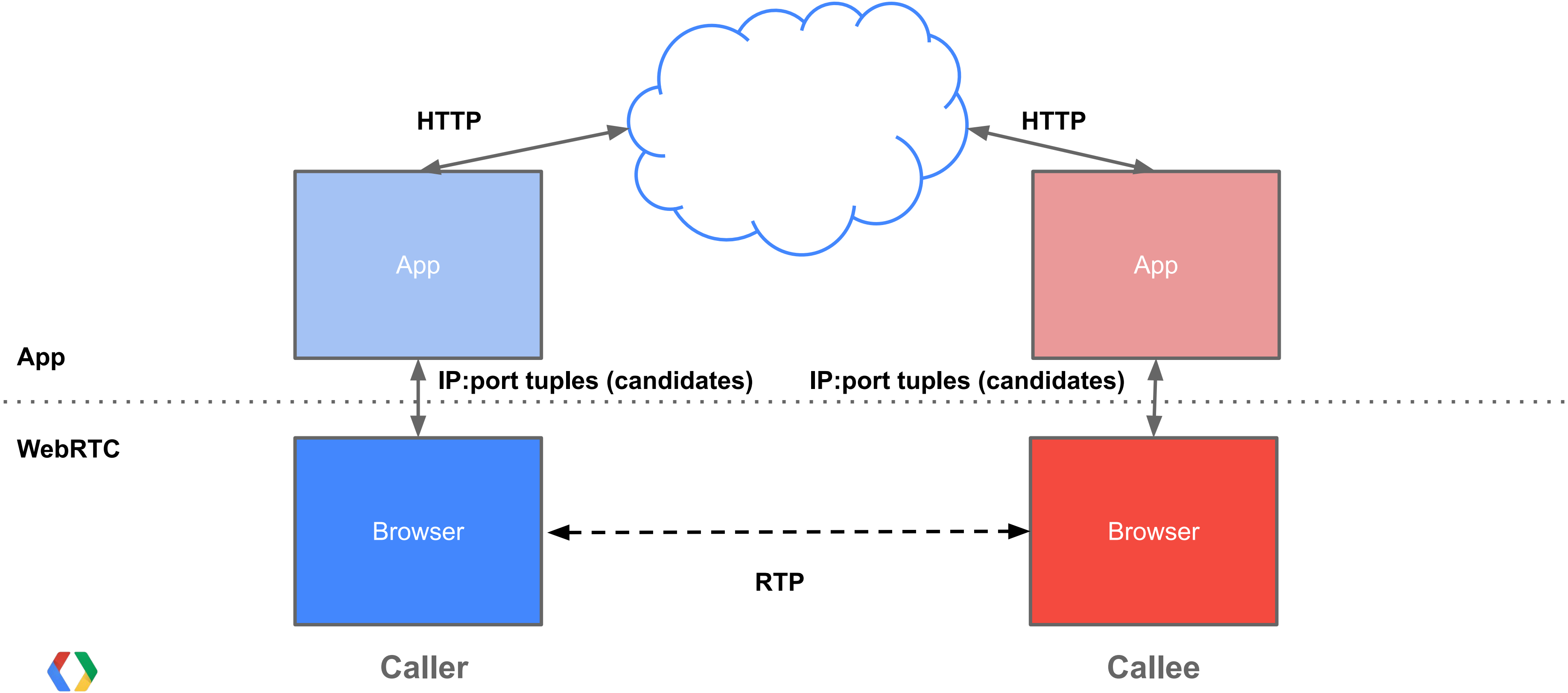
# WebRTC, mDNS and IP privacy

Justin Uberti

IETF PEARG Research Group Interim Meeting
January 19, 2021

# WebRTC Call Setup

IP Address Exchange



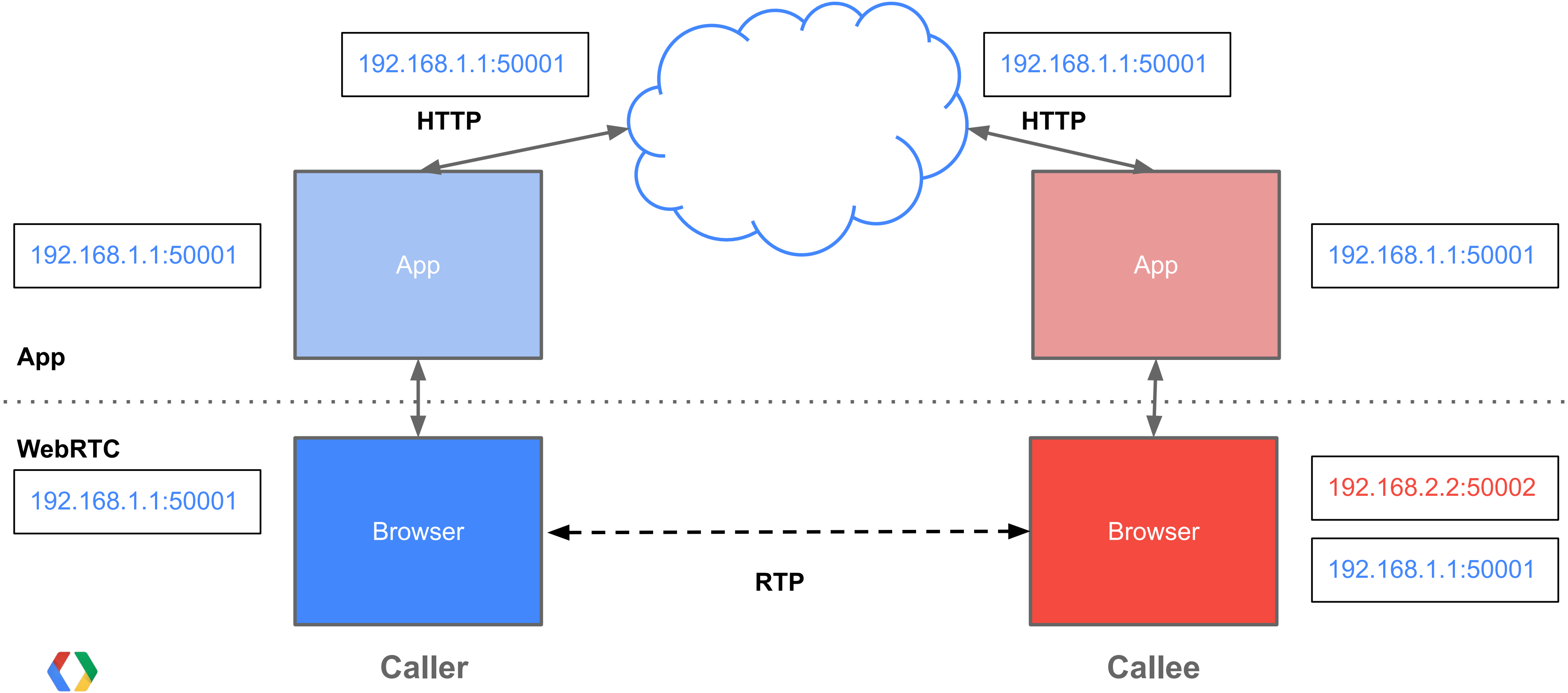
# WebRTC Call Setup

What is going on here?

- Each browser opens a UDP socket and gets an IP:port tuple (e.g. 192.168.0.1)
- The browser then calls the app to tell it about this tuple, known as a "candidate address".
- The app then uses XHR or similar to send the candidate to the calling service, who routes it to the remote client (via hanging GET, etc)
- The remote app passes the candidate to the browser, and also does the same with its own local candidate.
- Now that the peers have exchanged addresses, they can try to establish direct connections with each other.

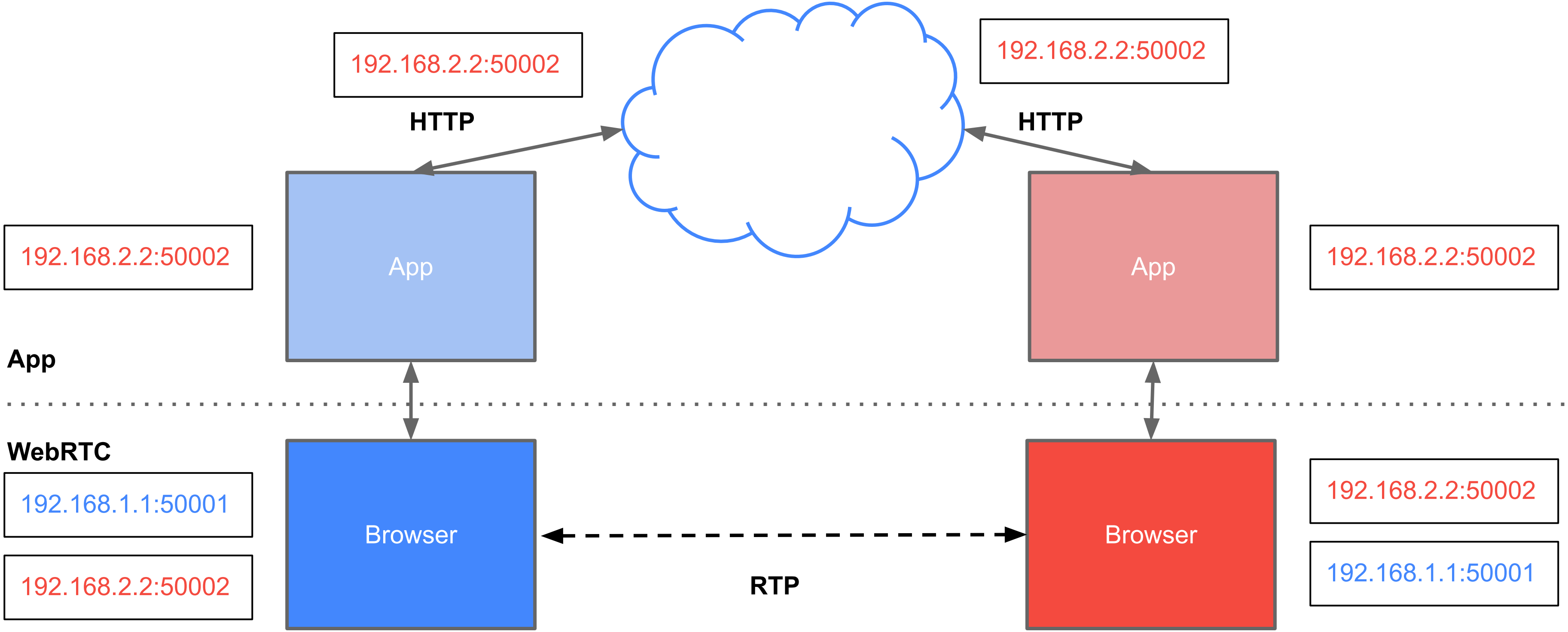
# WebRTC Call Setup

IP Address Exchange



# WebRTC Call Setup

IP Address Exchange



Caller

Callee

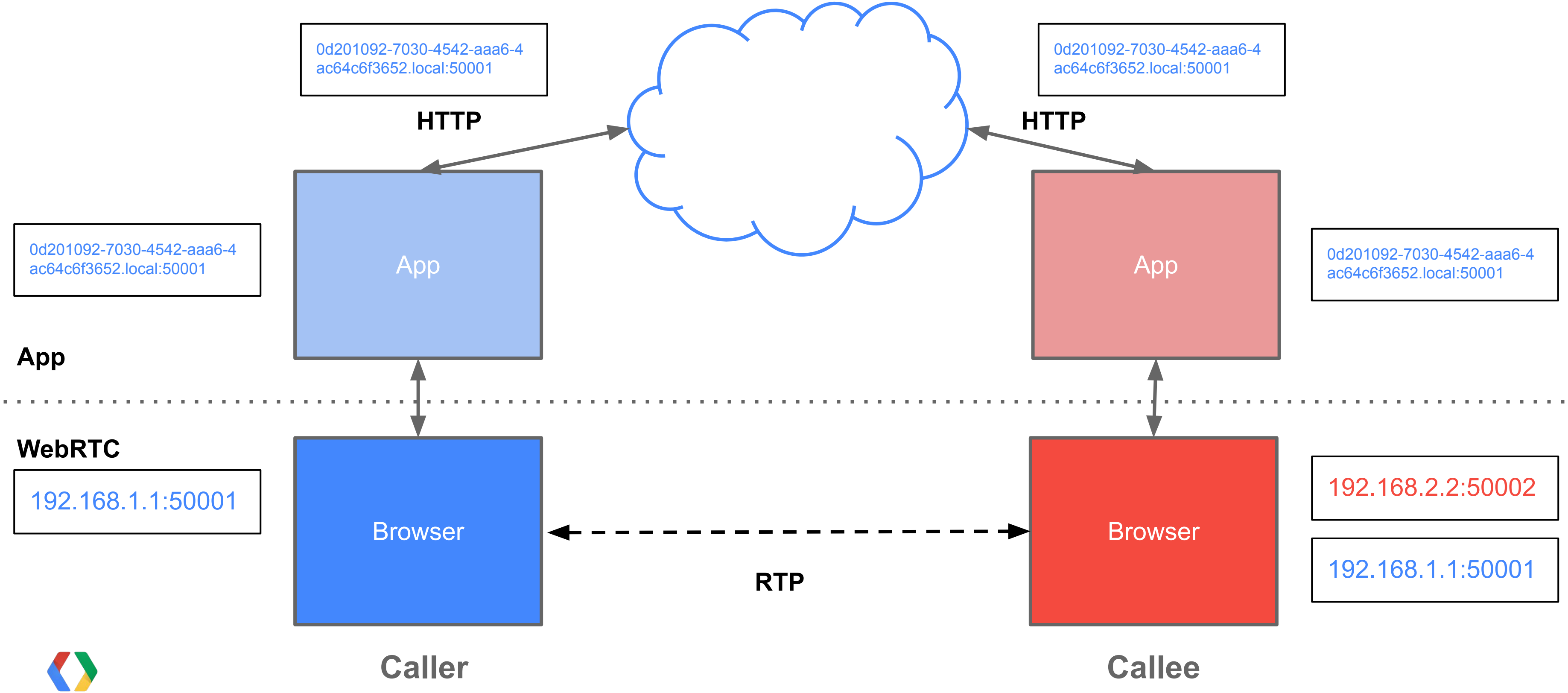
# Privacy Challenges

App has direct access to local IP

- Because the IP addresses are passed through the app, malicious apps can use the IP for tracking or other nefarious purposes
- As a local (typically RFC1918) address, this is an address the app doesn't usually have access to
- Hiding these addresses prevents direct connections on the same LAN
- What to do?

# WebRTC Call Setup with mDNS

## New Address Exchange



0d201092-7030-4542-aaa6-4ac64c6f3652.local:50001

HTTP

0d201092-7030-4542-aaa6-4ac64c6f3652.local:50001

HTTP

0d201092-7030-4542-aaa6-4ac64c6f3652.local:50001

App

App

0d201092-7030-4542-aaa6-4ac64c6f3652.local:50001

App

WebRTC

192.168.1.1:50001

Browser

Browser

192.168.2.2:50002

192.168.1.1:50001

RTP

Caller

Callee

# WebRTC Call Setup with mDNS

IP wrapped by mDNS

- Each browser registers a new UUID.local mDNS name that corresponds to its IP
- The browser then gives the mDNS name and port, rather than IP, to the app
- When the remote browser gets the mDNS name, it tries to resolve it to an IP.
- If it succeeds, it connects as usual to the resolved IP and supplied port.
- If it fails, the peer probably wasn't reachable at that address anyway!
- App does not have access to the resolved IP

# Summary

- The mDNS technique [1] effectively is a `W(K, IP)` wrap function, where K is known to all browsers on the local LAN, but not the app
- The browser will 'wrap' before passing to the app and 'unwrap' before trying to connect
- In situations where mDNS is not supported, IPs can be directly encrypted [2] based on a K pushed to all local browsers (via Chrome enterprise policy, etc)

1. https://tools.ietf.org/html/draft-ietf-mmusic-mdns-ice-candidates
2. https://tools.ietf.org/html/draft-wang-mmusic-encrypted-ice-candidates