Reservation & Sharing

- Who gets to access a device?
- Who gets to modify a device?
  - How are other accessors affected?
  - How are they notified of this?
- How do you set up a secure call?

Who gets to access a device?

- Types of access possible:
  - Exclusive (by default or via locking)
  - Shared with any other tab/app
  - Shared with other tabs/apps from the same-origin
  - Shared with “friend” apps (explicit sharing)
- What permissions requests surface to the user?
  - Only really matters if the user isn't for some reason selecting the input device
  - Should the user be apprised that a source is already in-use?
  - Does sharing need to be explicitly granted?
  - How does an app know if the source is shared?

My thoughts

- Firefox implements sharing if the user gives permission
- Locking or an exclusivity constraint seems useful
- Pure exclusive seems overly-restrictive
- Reasonable alternative: exclusive default, permissive if a constraint says so (could be an optional constraint).
- In firefox, since it doubles as selection, same-origin doesn't surface until we support persistent permissions
- Knowledge of sharing: event?

Who gets to modify a shared device?

- First user/Everyone/??
  - I think it has to be everyone
    - There are minor privacy concerns here – exclusive access solves them
- Conflicts
  - Can you 'lock' a parameter that's critical to you?
    - Deadlocks?
  - Can someone modify a parameter that was a “mandatory” to you?
- How do you know when someone modified it?

Security and Trust Model

- Default is the app gets access to the bits
  - Could send them anywhere via a peerconnection
    - “Local photobooth” app could be streaming your camera to the site/anyone. No privacy/blackmail/spying protection here...
  - Could access raw bits too look for “interesting” data and then upload it somewhere
    - Lots of flesh-colored pixels, image recognition, voice recognition
    - Note that this is actually also a really useful functionality
      - Face login
      - Voice commands

Security (cont)

- How do you set up a (“true”) secure call?
  - Protection from the app itself
    - Blocking access via canvas/Web audio/etc
      - Tainting?
  - Protection from another tab sharing access to the device
    - Need a way to know if someone is sharing the device (to be able to warn the user) and perhaps block new accesses (if they can be made without the user's permission).
- Do we punt and say “true secure calls require trusting the app with the bits” and just worry about sharing?