getCapabilities

Privacy & Security Concerns

User Consent

- ~33 bits needed to uniquely identify a user
- Most browsers already expose 20 bits

- Conclusion:
  getCapabilities MUST trigger a consent dialog

UI Requirements

- What is the user "consenting" to?
- Do we place requirements on the UI for the consent dialog:
  - Eg: show previews from all cameras returned by getCapabilities?
  - How will switching between sources work? (Content vs. Browser chrome)

Permissions

- <iframe> trickiness
  - Ad iframe embedded in trusted site
  - Worse: trusted site embedded in others?
- Tying permissions to origin is *NOT* great
  - We need to associate them with sessions
  - Possible to tie with identity proposal

API considerations

- What is the *minimum* amount of information that we need to expose?
- We should be wary of an explosion in the number of “profiles”
- Keep the API simple for those who don’t need capabilities but make it possible to build sophisticated UIs

Summary

- We need something that looks like getCapabilities, but only for sites that the UA can reasonably assume the user trusts

- The Devil is in the Details!