WebRTC IP Address Privacy

ekr@rtfm.com

Background: ICE

- RFC 5245 ICE gathers all the clients IP addresses for each interface
  - Host (local IP)
  - Server reflexive (apparent IP from STUN server)
  - Relayed (IP assigned by TURN server)
- So the Web server learns:
  - Local (RFC 1918) address
  - Public addresses even behind a VPN

Privacy Impact

- Increased fingerprinting surface
  - Doesn't help identify clients whose public IP addresses change (private IP changes too)
  - Distinguish people behind the same NAT
- Identify IP addresses "hidden" by VPNs
  - Should only happen with "split" VPNs -- but lots of people run them
  - VPNs already known to be insufficient here [ARF+12][PVT+15]

Privacy Impact (2)

- Identify IP addresses "hidden" by proxies
  - STUN traffic, over UDP, will skip a HTTP proxy
  - Not a bad thing... unless you are trying to hide
  - People hiding behind such proxies constitute a nontrivial fraction of abuse scenarios
  - Use of WebRTC to detect such cases is trending upward

Security Impact

- Discover address on local subnet
  - Potential input to firewall bypass attacks
- But there are other ways to do this
  - E.g., XHR to various local addresses

Potential Options

- Do nothing
- Indicator when WebRTC is being used ("eye of Sauron")
- Consent for any WebRTC network access
- More restricted ICE gathering
  - By default or as options
- Extensions to disable/restrict WebRTC

Restricted ICE gathering

- General idea: only publicly visible addresses
- Chrome (from 43 onward)
  - Bind host candidate to 0.0.0.0
  - Publish only srflx/relay candidates
  - Opt-in up to 46; making default in 47
- Firefox (from 43 onward)
  - Bind to addr used for "default" route
  - Publish only srflx/relay candidates (and stomp raddr)
  - Currently opt-in

What about restricted defaults?

- One proposal: do restricted gathering unless consent otherwise granted
  - Implicitly for camera/microphone
  - Explicitly for data communications
- Big question: what is the impact on data-only LAN scenarios?
  - Falls back to TURN if NAT doesn't hairpin
  - How often does this happen
- Still need to take measurements

Collateral damage

- Pretty much everything still works with restricted gathering, except demo pages... because no STUN/TURN
- This is unfortunate
- **Proposal**: emit localhost candidate for these cases
- **Challenge**: detecting these cases

Collateral damage (2)

- Don't want to emit localhost in cases where STUN/TURN is unnecessary (e.g. Hangouts)
- **Proposal**: (RTCConfiguration)
  - `iceServers: undefined` -> localhost candidate
  - `iceServers: []` -> no localhost candidate