WebRTC: API Impacts of Security

Interim Meeting; February 2012

Eric Rescorla

ekr@rtfm.com

Assumption: You remember what happened before lunch

- What's the implication for the W3C WebRTC WG?

Permissions Type API (S 5.2)

- Need some way to indicate what kind of permissions you want
  - E.g., long-term versus short-term

API for Secure MediaStreams (S 5.3)

- Need details on how to specify that a server can't manipulate MediaStream
  - Not just for WebRTC
- See Randell Jesup's presentation

IP Location Privacy (S 5.4)

- New API to suppress ICE negotiation but allow candidate gathering
  - Idea is to get a head start but not reveal your IP address
- New API to use only TURN candidates only
  - Hide IP address entirely
  - Should be able to add non-TURN candidates later

Keying Material Policy (S 5.5)

- New API to control key lifetime
  - Force use of a new key on this call to avoid linkability
  - Make a long-term key to allow key continuity

New Identity-oriented APIs: Authenticating Party

- Need to specify the IdP choice
  - Need a dominance model (for browser versus JS) settings
- What needs to be communicated:
  - One (or more?) IdP domain/protocol pairs
- Should this be done in configurations or via an explicit API call?

A plea for sanity on the configuration parameters

`new`PeerConnection("STUN 203.0.113.2:3478", signalingCallback);

- Please please please make the parameters be a JS structure

New Identity-oriented APIs: Relying Party

- Need some way to get the identity assertion value

```
{
  "idp":{
       "domain": "example.org"
       "protocol": "bogus"
   },

   "identity": {
          "name" : "bob@example.org",
          "displayname" : "Bob"
    },
}
```