RTCWEB Security Architecture Update

Eric Rescorla

Mozilla

ekr@rtfm.com

COMSEC

- MUST NOT for SDES
- Mandatory cipher suites
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - SRTP_AES128_CM_HMAC_SHA1_80
- Implementations SHOULD favor cipher suites which support PFS over non-PFS cipher suites.
- Note: ECDHE still not standards track in TLS
  - But we are looking at it in TLS

Identity

- Convert `postMessage()` to a named `MessageChannel`
  - This removes the need to have an `rtcweb://` origin
- Remove displayname field
- Clearer rules about identity string format
- Slightly restructure IdP verification response to reduce depth
- Rules for sanitizing IdP domain names

What's next?

- Martin has some comments about IdP based on Mozilla's implementation
- Plan is to address those and then be ready for another WGLC.