Security documents rundown

draft-ietf-rtcweb-security-05

draft-ietf-rtcweb-security-arch-07

Eric Rescorla

ekr@rtfm.com

IETF 87

July 30, 2013

Overview

- Got a lot of feedback
  - Tried to incorporate most of it
- Thanks to: Bernard Aboba, Harald Alvestrand, Richard Barnes, Dan Druta, Cullen Jennings, Alan Johnston, Hadriel Kaplan, Matthew Kaufman, Jim McEachern, Martin Thomson, Magnus Westerland.

Selected changes to `draft-ietf-rtcweb-security-05`

- Added privacy considerations section and discussion of IP location privacy and Tor
- Edited the SAS section to reflect Alan Johnston's comments
- Updated communications consent section to point to draft-muthu
- Added a section about malicious peers
- Added a section on screen sharing threats

Selected changes to

draft-ietf-rtcweb-security-arch-07

- Forbade use with mixed content (per Orlando)
- Added screen sharing permission reqts
- Added a requirement to surface NULL ciphers

Screen Sharing

- Screen sharing has some pretty serious security threats
  - But people really want it...

Proposed Screen Sharing Requirements

- Browsers MUST not permit permanent screen or application sharing permissions to be installed as a response to a JS request for permissions. Instead, they must require some other user action such as a permissions setting or an application install experience to grant permission to a site.
- Browsers MUST provide a separate dialog request for screen/ application sharing permissions even if the media request is made at the same time as camera and microphone.
- The browser MUST indicate any windows which are currently being shared in some unambiguous way. Windows which are not visible MUST not be shared even if the application is being shared. If the screen is being shared, then that MUST be indicated.

Null Ciphers

- The current specification requires you to call out null ciphers
- Martin Thomson suggests that we just ban them
- This sounds like a good idea to me

Next Steps

- Got some more minor comments
- Also realized I missed a few comments from before
- Expect a new version shortly after IETF