RTCWEB Security LC Comments (good parts version)

RTCWEB

Eric Rescorla

Thanks to

Bernard Aboba, Alan Johnston, Oscar Ohlsson, Martin Thomson, Justin Uberti, Magnus Westerlund, [Your name here]

Documents

- draft-ietf-rtcweb-security-04
- draft-ietf-rtcweb-security-arch-06

Overview

- Got a lot of good comments
- I agree with most of them
- I will prepare a new draft addressing all the comments
- These are the ones I think need discussion here

draft-ietf-rtcweb-security-04

Perfect Forward Secrecy (Aboba)

RTC-Web (this is a good idea for any communications security system) and this mechanism SHOULD provide perfect forward secrecy (PFS).

- Aboba asks 'Do we mean "SHOULD support" PFS or "SHOULD use"?'
- DTLS-SRTP supports PFS modes but SDES does not
  - EKT generally inherits the properties of the weakest channel it is used with
- Proposal: SHOULD USE PFS? Should this be a MUST with DTLS?

Name of the system (Westerlund)

- RTCWEB versus WebRTC
- Do I just do s/RTCWEB/WebRTC/?

draft-ietf-rtcweb-security-arch-06

Mixed content (Westerlund, Johston)

"It is RECOMMENDED that browsers which allow active mixed content nevertheless disable RTCWEB functionality in mixed content settings. [[OPEN ISSUE: Should this be a 2119 MUST? It's not clear what set of conditions would make this OK, other than that browser manufacturers have traditionally been permissive here here.]]" [§5.1]

- Browsers are moving to block active mixed content already
  - Chrome/IE already do
  - Under development for Firefox; target=Firefox 22.
- Proposal: ban use of WebRTC with mixed content entirely
- Alternate approach: refuse persistent permissions in mixed content settings
- Do we need to take this to W3C?

Linkage Issues (Westerlund)

- General model is to avoid creating a super-cookie
  - Not a requirement to stop sites from doing things they can do with cookies
  - Can't do much about fingerprinting :(
- Known linkage points
  - DTLS certificates/keys
  - CNAMEs
  - API fingerprinting
- Need to document things that link calls
- Am I missing other things?

Guy on the other end (Thomson)

> "This opens a new category of attack, one that I wasn't all that concerned about. Namely, the guy on the other end isn't trustworthy.
>
> To a large extent, peer authentication allows users to make their own assessments, but we have to acknowledge (and likely accept) that the other guy isn't necessarily trustworthy. I think that we can rule the age-old human problem out of scope, but perhaps we should be clear that we are doing so."

– Thomson

- I agree with this and will add text unless someone objects.

Screen Sharing (Uberti)

- Really important feature
- But turns out to be riskier than you think
  - Basically, blows up Same Origin Policy
  - `http://lists.w3.org/Archives/Public/public-webrtc/2013Mar/0024.html`
- I assume people still want this feature
  - ... even though maybe they shouldn't
- Proposal: add (shortened) discussion of risks and propose some UI reqts

How to talk about site authentication (Johnston)

Web sites whose origin we can verify (optimally via HTTPS, but in some cases because we are on a topologically restricted network, such as behind a firewall)" - what is the 2nd case - no verification? Verification using something other than HTTPS? [§3.1]

- Johnston writes: "what is the 2nd case - no verification? Verification using something other than HTTPS?"
- Idea here is supposed to be to accomodate firewalls or VPNs.
  - This has been discussed a lot but my text isn't clear, apparently
  - Suggestions?