draft-ietf-rtcweb-security-arch
draft-ietf-rtcweb-security

IETF 94

2nd RTCweb WG Session

Status

- Draft state: “Waiting for WG Chair Go-Ahead”
- Revisions suggested @ IETF 92 need to be included.
    - m=fingerprint: SHA-256 vice SHA-1
    - Nuke SDES holdover
    - Edit out WTF cipher suites
- github PRs:

– Adopt ECDSA
https://github.com/rtcweb-wg/security-arch/pull/33

Reviews

- AppsDir: http://tinyurl.com/qfl9ujy
  - **draft-ietf-rtcweb-security-arch**
  - **draft-ietf-rtcweb-security**
- SecDir: http://tinyurl.com/qy4rt9p
  - draft-ietf-rtcweb-security-arch

secdir “discuss” s4.1 Initial Signaling

- Alice is logged onto the calling service and decides to call Bob. She can see from the calling service that he is online and the calling service presents a JS UI in the form of a button next to Bob's name which says "Call". Alice clicks the button, which initiates a JS callback that instantiates a PeerConnection object. This does not require a security check: JS from any origin is allowed to get this far.

- Comment: Maybe the wording is unprecise, or if it is intended as I read it than I beg to disagree. There are several security concerns if that would be the case. Just a few examples, I am sure there are plenty more:
  1. Privacy concerns if you can trigger someone initiating a call
  2. Denial of service scenarios, creation of PeerConnections or the scenario of "the great cannon of China" comes to mind, in which you can let other people flood a recipient with call requests.

secdir “comment” s4.1

- In the following s/preferably over TLS/it SHOULD use TLS:
  - This message is sent to the signaling server, e.g., by XMLHttpRequest [XmlHttpRequest] or by WebSockets [RFC6455] preferably over TLS [RFC5246].
- If possible, I would even go for "MUST", but I am not sure about whether there are legitimate use cases that require non-TLS?

secdir “comment” s5.2

- Open issue encompassing the following three bullets:
- 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.

secdir “comment” s5.5

- Do we need to assert that the client provide UI information from which peer the current stream is coming from?
- Assuming you have 3 or more peers (A, B and C) in a meeting, can you avoid that B replays the voice of A in effect spoofing him to C on the application layer?

secdir “comment” s5.7.1

- Do you need to support UNICODE characters for identities [format]?
- Preferably, I would like to avoid such, as that could cause it's own set of potential problems with similar looking codepoints....

secdir “question” s6.3

- Section 6.3. states that "On the other hand, signing the entire message severely restricts the capabilities of the calling application, so there are difficult tradeoffs here.”
- Actually my assumption was that the entire signalling message would be signed. What are the implied restrictions that prevent that from happening? Is there a way we could allow for that?

secdir “comment” s6.4.2 IdP Well-known URI

- Assuming a server that does not host an IdP nor is aware of the special semantics of this "well-known URI".
- Would an attacker with access to this initially empty structure be able to create a working IdP and assert identities for the domain of that server that might supersede other 3rd-party IdP servers?

secdir “comment” s6.4.5.1/6.4.5.2

- It seems the text is suggestion that popup blocking and third party cookie blocking are not compatible with using an IdP. I would recommend a statement that sites SHOULD (MUST?) implement in a way that they still function with client side popup blocking and third party cookie blocking.

secdir “general”

- I wonder whether an IdP can by providing the identity assertions for the users determine a very detailed record of all call metadata (time, src, dst, ...) of all communications for a user. Are there any abstraction mechanisms we could deploy to limit that exposure to the IdP? On the other hand, is the identity assertion linked to a system time, to avoid later replay attacks?