RTCWEB Security Drafts

Bangkok, Thailand

November 8, 2018

Current Status

- draft-ietf-rtcweb-security and draft-ietf-rtcweb-ip-handling are ready to go, modulo an update to ICE bis
- draft-ietf-rtcweb-security-arch has some ambiguities that need clarification

Issue 1: Invalid Identity in Initial Answer (§5.1.4)

- Current text says to treat the same way as invalid identity in Initial Offer
- This doesn't really make sense, since offers can be rejected and answers can't
- Proposal: adjust language to say the session must be torn down if identity verification fails

Issue 2: Invalid Identity in Updated Offer (§5.1.5)

- Text does not say what to do if validation fails
- Since the session already exists, we have three choices:
  1. Reject the Offer
  2. Terminate the Session
  3. Explicitly leave it up to the application
- Suggestion: Terminate the Session. Something fishy is going on.

Issue 3: Invalid Identity in Updated *Answer* (§5.1.5)

- Kind of the same problem as previous issue, except that JSEP doesn't have a way for answerer to roll back to previous state if the answer is bad
  - This would be hard to add at this point
  - And it's probably not what we want anyway
- Proposal: Add explicit text that says the session terminates.

Issue 4: DTLS MTI Version (§6.5)

- Current text says "All implementations MUST implement DTLS 1.0"
- RFC 7525: "Implementations SHOULD NOT negotiate DTLS version 1.0"
- draft-ietf-tls-oldversions-deprecate: "Implementations MUST NOT negotiate DTLS version 1.0"
- Unless I'm being dense, this seems out of sync.
- But what *is* the right answer?

Issue 5: A-label or U-label in Identities (§8.1)

- Text says domain portion of identity is an IDN, citing RFC 5890
- RFC 5890 defines two encodings:
  - A-label:
    `xn--22c6dm4a2dze.xn--42cl2bj2hxbd2g.xn--12co0c3b4eva.xn--o3cw4h`
  - U-label: ข้อมูล.ทีเอชนิค.ธุรกิจ.ไทย
- Recommendation: U-label

Issue 6: Identity User Portion Escaping (§8.1)

- Current text says that usernames that contain "@" characters should escape illegal characters.
  - It does not define how this escaping is to take place
  - Example implies URI percent-encoding
- Two options:
  1. Normatively cite percent encoding, require it for both "@" and "%"
  2. Clarify that we mean "implementation-dependent transformation"
- Suggestion: option 1: it allows user agents to perform unescaping before presenting to users
  - Would need to add guidance about rendering multiple "@" signs

Next Steps

- I plan to hold the documents for update until the ICE references have been updated
- All three documents will go into IETF LC together