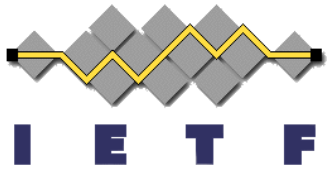
CLUE Working Group

Daniel Burnett
Roni Even
Paul Kyzivat

http://datatracker.ietf.org/wg/clue/charter/



Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda bash - Monday

13:00 CLUE Status Update (Chairs, 20)

13:20 CLUE protocol (Simon Romano, 20)

13:40 CLUE Signaling (Rob Hansen, 30)

14:10 Mapping RTP streams to CLUE media captures (Roni Even, 15)

14:25 End

Document Status

- CLUE framework in draft-ietf-clue-framework-22 went to the IESG, there were comments from the AD waiting for response
- An XML Schema for the CLUE data model in draft-ietf-clue-data-model-schema-10 submitted after the WGLC.
  - Open issue – do we need an IANA registry for the policy token?
- Need volunteers to review the documents.
  - Protocol (in WGLC)
  - Signaling
  - RTP mapping

Framework security

- "Thus, it is RECOMMENDED that an MCU implementing the protocols necessary to support CLUE, follow the security recommendations specified in the conference control protocol documents.“
  - The specific documents need to be listed here, assuming RFC 4579 is not the only one to be mentioned.
- "Thus the security mechanisms recommended for SIP [RFC3261], including user authentication and authorization, SHOULD be followed.“
  - Given that implementations will need to be updated to support CLUE, what is the rationale for having user authentication and authorization be optional? What are the cases where allowing an unauthenticated or unauthorized participant to join a telepresence session would be considered acceptable?

Framework security

- "In addition, the media is based on RTP and thus existing RTP security mechanisms SHOULD be supported, and DTLS/SRTP MUST be supported. Media security is also discussed in [I-D.ietf-clue-signaling] and [I-D.ietf-clue-rtp-mapping].“
  - I think it's worth pointing out in this document that DTLS/SRTP is required to use for CLUE-controlled m-lines. Also, I just did a quick skim of draft-ietf-clue-rtp-mapping and didn't see anything in there about media security.
  - My view – maybe reference RFC7202 (srtp-not-mandatory)

Framework security

- "A separate data channel is established to transport the CLUE protocol messages. The contents of the CLUE protocol messages are based on information introduced in this document. The CLUE data model [I-D.ietf-clue-data-model-schema] defines through an XML schema the syntax to be used. Some of the information which could possibly introduce privacy concerns is the xCard information as described in section 7.1.1.11. In addition, the (text) description field in the Media Capture attribute (section 7.1.1.7) could possibly reveal sensitive information or specific identities. The same would be true for the descriptions in the Capture Scene (section 7.3.1) and Capture Scene View (7.3.2) attributes. One other important consideration for the information in the xCard as well as the description field in the Media Capture and Capture Scene View attributes is that while the endpoints involved in the session have been authenticated, there is no assurance that the information in the xCard or description fields is authentic. Thus, this information MUST NOT be used to make any authorization decisions."

Framework security

- I don't think it's enough to point out that sensitive data can be sent back and forth with CLUE and that it shouldn't be used for authorization decisions. Is there some guidance that can be given about minimizing the amount and sensitivity of data to be sent? Are there certain xCard fields that endpoints should avoid sending? Some of this is obviously dependent on context and whether the participants in a conference know this information about each other already, but it's still worth mentioning how to mitigate the risks of sharing more data or more sensitive data than is necessary for the purposes of supporting a telepresence session. This might imply additional text in 7.1.1.10 as well.

Framework security

- "Thus, it MUST be possible for the endpoints to establish a channel which is secure against both message recovery and message modification. Further details on this are provided in the CLUE data channel solution document."

  There are no details about how the data channel is secured in draft-ietf-clue-datachannel (which should be cited here if it's going to be referenced). Nor are the details in draft-ietf-rtcweb-data-channel, but rather they are in draft-ietf-rtcweb-security-arch and draft-ietf-rtcweb-security.

  Furthermore, the details provided in draft-ietf-rtcweb-security-arch and draft-ietf-rtcweb-security explain the situation for rtcweb, where the endpoints rely on identity providers to authenticate each others' identities. IdPs are not specifically included in the CLUE architecture and, as noted above, the SIP authentication mechanisms are optional -- so how is it that the CLUE data channel is actually secured against an active MITM?