

Formal Analysis Triage Panel

<https://mailarchive.ietf.org/arch/msg/tls/RupKEHeJdAzxpNEZnRgerk4en1c/>

[TLS] Completion of Update Call for RFC 8773bis

Joseph Salowey <joe@salowey.net> | Tue, 23 January 2024 15:50 UTC | [Show header](#)

The working group last call for RFC8773bis has completed (draft-ietf-tls-8773bis). There was general support for moving the document forward and upgrading its status. However, several working group participants raised the concern that formal analysis has not been conducted on this modification to the TLS protocol. We should at least have consensus on whether this document has the required analysis before upgrading it, but we also need a more general statement on this requirement since the TLS working group currently does not have a policy for what does and does not need formal analysis or what constitutes proper formal analysis.

The chairs are working on a proposal for handling situations like this that we plan to post to the list in a week or so.

Thanks,

Joe, Deirdre, and Sean

[TLS] Completion of Update Call for RFC 8773bis

Joseph Salowey <joe@salowey.net> | Tue, 23 January 2024 15:50 UTC | [Show header](#)

The working group last call for RFC8773bis has completed (draft-ietf-tls-8773bis). There was general support for moving the document forward and upgrading its status. However, several working group participants raised the concern that formal analysis has not been conducted on this modification to the TLS protocol. We should at least have consensus on whether this document has the required analysis before upgrading it, but we also need a more general statement on this requirement since the TLS working group currently does not have a policy for what does and does not need formal analysis or what constitutes proper formal analysis.

The chairs are working on a proposal for handling situations like this that we plan to post to the list in a week or so.

Thanks,

Joe, Deirdre, and Sean

Proposal: triage, then maybe analyze

Triage panel: rotating group who have volunteered to give preliminary triage of proposed changes to TLS 1.3¹ and *whether* they need updated or new formal analysis (of any kind), and an estimate of the scope of work such an analysis would entail

¹ 1.3 has the most robust analysis; we'll see about other versions

Proposal: triage, then maybe analyze

At document/change adoption call, chairs email the triage panel, bring summarized analysis to the WG as part of the adoption discussion.

If the triage panel recommends analysis w/ scope, and the WG accepts, the WGLC for that document is blocked on the completion of formal analysis.

If analysis was not recommended, but the document changes significantly between adoption and pre-WGLC, a second look can be requested, and proceed as above ('last chance').

Proposal: triage, then maybe analyze

If the working group agrees to proceed, the formal analysis triage panel consults on farming out the meat of the analysis work (either to their teams or to students they supervise, etc.)


Triage panel membership can be refreshed on a regular schedule or on an as-needed basis (IETF meetings can be a regular check-in.)

‘What kind of formal analysis?’

Not just Tamarin

Our panel of experts can suggest specific approaches: building on existing work, new models, pen and paper game proofs, computational models for small pieces, symbolic model for higher level pieces, etc

Checking against existing work, but not being beholden to only build on existing work

: Maintain the high degree of cryptographic assurance in TLS 1.3 as it evolves

Thoughts?

Formal Analysis Triage Panel