Formal Analysis Triage Panel

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

Formal Analysis Triage ~~Panel~~

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

Formal Analysis Triage Team

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

Formal Analysis Triage Team (FATT)

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 hea

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

https://datatracker.ietf.org/doc/draft-ietf-tls-8773bis/

[TLS] Completion of Update Call for RFC 8773bis

Joseph Salowey <joe@salowey.net> | Tue, 23 January 2024 15:50 UTC | Show hea

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

https://datatracker.ietf.org/doc/draft-ietf-tls-8773bis/

Mechanism: triage, then maybe analyze

Triage panel: rotating group who have volunteered to give preliminary triage of proposed changes to TLS 1.3[1] 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

Mechanism: 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’).

Mechanism: 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

First try: 8773bis [HARD MODE]

Workgroup: Network Working Group
Internet-Draft: draft-ietf-tls-8773bis-02
Published: 7 July 2024
Intended Status: Standards Track
Expires: 8 January 2025

R. Housley
Vigil Security

TLS 1.3 Extension for Using Certificates with an External Pre-Shared Key

Abstract

This document specifies a TLS 1.3 extension that allows TLS clients and servers to authenticate with a combination of a certificate and an external pre-shared key (PSK).

8773bis

- Already went through adoption, wglc; out-of-band FATT review
- FATT recommended:
  - More clarity in the document on intended security goals
  - Further analysis to check especially the authentication properties, symbolic analysis tools would be suitable
- Document hasn’t changed yet
- Russ and Usama collaborating on ProVerif model?
  - If not accurate, we chairs can collaborate on finding participants and scoping the work
- No further consensus calls…yet

Q: Why isn’t the FATT discussion radically transparent?

- Modelled on peer review for academic submissions
- Reviewers confer with each other, agree on broad feedback, feedback is delivered to WG
- Everything proceeds as usual on the list (including whether to adopt the recommendations)
  - Including the ability to respond, address, or not, any discussion by any FATT participant
- Debate happens on the list after the FATT feedback is delivered
- So far this process has been:
  - An email from the chairs
  - The FATT participants (eventually) reply
  - Chairs consolidate responses and send to list
  - That’s it

Thoughts?

Formal Analysis Triage Panel