TLS FATT

Latest Process Description

https://github.com/tlswg/tls-fatt

- Incorporates feedback since the past meeting, including mailing list, interim meeting, Draft raft-rsalz-tls-analysis
- Much better description, but still a work in progress

Formal Analysis Triage Team (FATT)

- Membership is public available in TLS repo
- Membership managed by chairs with working group input
  - Membership questions - contact chairs
- “Ongoing” Design Team ++
  - Exists for the life of TLS 1.3 (and perhaps beyond)
- Deliberations of the FATT are private, output is input into WG consensus process
- “Point Person” assigned to each draft

Integration with Working Group Process

1. After WG adoption
    a. FATT is consulted to see if change should have additional security analysis. Results like:
        i. ‘nothing required’
        ii. 'pen-and-paper proof can be updated'
        iii. 'a formal methods model using a specific tool ought to be done'
2. At WGLC (if something required)
    a. Is analysis analysis sufficient
    b. Input to WGLC comments

Ongoing Discussion

- Getting Analysis Done
  - FATT can make suggestions
  - UFMRG
    - Looking at ANRW type publication and conference for Protocol Analysis
    - Improving tools to make them more accessible
  - Other ideas welcome
- Making Analysis go More Smoothly
  - What should a draft provide to facilitate analysis
    - What are the required security properties