Formal Analysis Triage Team (FATT) Report
draft-ietf-tls-8773bis

Liaison: Britta Hale

Main idea of draft:
Use PSKs in TLS (including early data) with claimed resultant quantum resilience

Formal Analysis Triage Team (FATT) Report
draft-ietf-tls-8773bis

- Requested 8773 reviews from researchers in the topic area to obtain feedback on whether a security analysis is needed or not
- Reviewers from both cryptographic computational and symbolic analysis areas
- All reviewers have published work related to TLS (and potentially also TLS PSK modes), i.e., very relevant expertise

Reviewers:

- Dr. Benjamin Dowling
- Dr. Felix Günther
- Dr. Thom Wiggers
- Dr. Jonathan Hoyland

- The report provides an aggregate of review comments, quoted directed wherever possible and minimally paraphrased when not, appropriately notated for each type, for WG transparency

- Responses are semi-anonymous: all reviewer names are listed, but quotes are not directly attributable to any specific reviewer

- Reviewers have not been asked to review the aggregate report
  (both to limit review burden and to ensure protect from concurrence attribution)

Reminder: DO NOT contact reviewers directly.

If they wanted to engaged in IETF processes, they would (and have been invited). Review contribution in the FATT is highly contingent on the IETF making the experience pleasant for those volunteers.

Any questions and comments should go to the Liaison for clarification.

Net summary:

- Reviewers shared similar concerns across both computational and symbolic analysis approaches
- **Positives**: 8773 is unlikely to introduce vulnerabilities or need for analysis to *traditional* TLS
- **Negatives**: More severe concerns about 8773 under the claims for quantum resilient security, i.e., there were strong concerns about the security claimed by the solution under its stated threat model:
    1. Claims about authentication were not substantiated
    2. Claims about quantum resilient security were not substantiated given lack of clarity in PSK generation (not specified – would a PSK be derived from a traditional session suffice?)
    3. Security guarantees under quantum adversary are unclear: Resulting security is notably not "TLS Security" under a quantum attacker when PSK reuse is allowed across sessions and use types (i.e., no key separation under a quantum adversary)
    4. Grounding for claims about TLS security (or general security) under a quantum adversary is unclear, since PSKs are allowed to be owned and accessed by multiple members beyond the two communicating parties
    5. It is not clear if the guarantees meant are for hybrid or not and, if hybrid, what form

As the FATT recommendation based on the reviews, one of two potential courses of action was recommended:

1. Reduce or remove the motivation and security claims in the document on quantum resilience of 8773, such that the functional inclusion of a PSK is an offered functional attribute only and not a point of reliance for content confidentiality. This option can move ahead without further analysis.

2. Keep the security claims and current motivation, which includes protections from quantum adversaries. This option requires analysis.

In both cases, 8773 should provide improved clarity on the authentication properties associated with and expected from the PSK, PSK provenance, PSK reuse restrictions, and 0-RTT use of the PSK, as well as downgrade allowances or restrictions from sessions using 8773 to standard TLS.

As the FATT recommendation based on the reviews, one of two potential courses of action was recommended:

1. Reduce or remove the motivation and security claims in the document on quantum resilience of 8773, such that the functional inclusion of a PSK is an offered functional attribute only and not a point of reliance for content confidentiality. This option can move ahead without further analysis.

2. Keep the security claims and current motivation, which includes protections from quantum adversaries. This option requires analysis.

In both cases, 8773 should provide improved clarity on the authentication properties associated with and expected from the PSK, PSK provenance, PSK reuse restrictions, and 0-RTT use of the PSK, as well as downgrade allowances or restrictions from sessions using 8773 to standard TLS.

Net summary:

- Reviewers shared similar concerns across both computational and symbolic analysis approaches
- **Positives**: 8773 is unlikely to introduce vulnerabilities or need for analysis to *traditional* TLS
- **Negatives**: More severe concerns about 8773 under the claims for quantum resilient security, i.e., there were strong concerns about the security claimed by the solution under its stated threat model:
    1. Claims about authentication were not substantiated
    2. Claims about quantum resilient security were not substantiated given lack of clarity in PSK generation (not specified – would a PSK be derived from a traditional session suffice?
    3. Security guarantees under quantum adversary are unclear: Resulting security is notably not cker when PSK reuse is allowed across sessions and use quantum adversary).
    4. ity (or general security) under a quantum adversary is unclear, since PSKs are allowed to be owned and accessed by multiple members beyond the two communicating parties
    5. It is not clear if the guarantees meant are for hybrid or not and, if hybrid, what form

Draft has been revised since the reviews to make clear that 1) the PSKs do not provide authentication, and 2) the requirement for quantum-resilient PSK generation and distribution methods

Net summary:

- Reviewers shared similar concerns across both computational and symbolic analysis approaches
- **Positives**: 8773 is unlikely to introduce vulnerabilities or need for analysis to *traditional* TLS
- **Negatives**: More severe concerns about 8773 under the claims for quantum resilient security, i.e., there were strong concerns about the security claimed by the solution under its stated threat model:
    1. Claims about authentication were not substantiated
    2. Claims about quantum resilient security were not substantiated given lack of clarity in PSK generation (not specified – would a PSK be derived from a traditional session suffice?)
    3. Security guarantees under quantum adversary are unclear: Resulting security is notably not "TLS Security" under a quantum attacker when PSK reuse is allowed across sessions and use types (i.e., no key separation under a quantum adversary)
    4. Grounding for claims about TLS security (or general security) under a quantum adversary is unclear, since PSKs are allowed to be owned and accessed by multiple members beyond the two communicating parties.
    5. It is not clear if the guarantees meant are for hybrid or not and, if hybrid, what form

The draft states that it offers TLS security against HNDL attacks.
However, given the PSK reuse and group use, under a quantum attacker the resultant TLS does not provide “TLS security” – it provides a form of group-like static key protection without the FS guarantees TLS now provides, key separation, nor uniqueness of session keys.

This is not an issue with group PSKs under traditional attackers for the obvious reason that the rest of the TLS handshake ensures unique client-server channel keys, but it is an issue under a quantum attacker which is what this draft is claiming security against.

Potential avenues to address this:

- remove PSK reuse and group option, to align the draft security more closely to TLS expected security under a quantum threat.

OR

- adjust design rationale and guarantees to remove interpretation of TLS security under a quantum attacker (focusing on draft security under traditional attackers and modifying to looser, non-TLS quantum resilience guarantees).

Author preference for keeping both PSK reuse and group options.

Corresponding FATT recommendation → obtain analysis and match security claims in the draft to corresponding provable security model.

Discussion