IETF Formal Analysis Triage Report of draft-ietf-tls-8773bis

By IETF FATT Liaison Britta Hale

Intent: The intent of this summary document is to inform IETF decisions on whether to solicit a cryptographic analysis for draft-ietf-tls-8773bis.

Content and Scope: This summary is for draft-ietf-tls-8773bis (henceforth referred to as "8773". This summary combines 8773 reviews from researchers who have performed prior analyses of TLS, especially analyses that modeled use of the PSK, and include researchers across the span of symbolic or computational analysis. These reviews should not be taken to constitute a detailed cryptographic analysis in themselves but are rather the combined expert review opinions of several researchers.

The content of this document is an aggregation of quotes directly from the researchers listed on the Reviewer List and summary of more informal inputs; however, the reviewer source of any given quote has been anonymized to refrain from attribution, following the intention of the FATT.

The reviewers have not been asked to review the final report as a whole nor the comments of other reviewers. This is to minimize the investment requirement for voluntary reviewer contributions, especially from those outside of the IETF. All expert reviews are greatly appreciated by the IETF and both the promised pseudo-anonymity and time investment of the reviewers will be respected.

Use Restrictions: Any questions should be directed to the IETF FATT Liaison for 8773; none of the researchers listed on the Reviewer List are to be contacted directly regarding this unless they first choose to participate in the IETF on the topic of 8773.

8773 Summary:
The document describes a mechanism for a single TLS 1.3 handshake to utilize both a PSK and standard certificate authentication. The threat model and security goal of this mechanism is to "protect today's communications from the future invention of a large-scale quantum computer"; specifically providing protection of content encryption in such a context, a.k.a. security against "harvest-now decrypt-later" attacks. The draft generally[1] describes authentication as based on existing certificates and digital signatures, and the PSK use is intended to run in tandem with ephemeral ECDH, so the security intent of the draft is for use in the context of a *future* quantum adversary but does not aim to provide authentication (entity or data authentication) guarantees for a context of a *contemporary* quantum adversary.

---

[1] See Concrete Recommendations for a clarity recommendation.

FATT Summary:
Reviewer comments highlighted that the 8773 technical changes to TLS through use of PSK are unlikely to introduce vulnerabilities to TLS in its current form, which should allay concerns from developers who rely on TLS security as-is and may have reservations about issues introduced by 8773. I.e., the functionality change introduced by 8773 did not raise much concern for present use of TLS and reviewers generally thought that no new analysis would be required assuming the traditional TLS threat model with assumptions that security is provided by the normal TLS aspects (vs 8773).

However, reviewers widely emphasized concerns about the security claims of 8773, and whether security is in fact achieved under the threat model posited in 8773. Ambiguities on what authenticity could be claimed through use of the PSK, PSK provenance and its effect on harvest-now-decrypt-later attacks, and reservations about the clarity of the intended security model were commonly emphasized. The reviewers were in general consensus that to make security claims in the document, new analysis would be required.

As the FATT recommendation based on the reviews, there are two potential courses of action that could be undertaken:

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.

Detailed comments:
Notation used in this report:
# Notates direct reviewer quotes.
* Notates indirect reviewer quotes. Direct quotes have been included wherever possible, but some input needed to be paraphrased for formality.
All other discussion can be taken as summary combining the input of various reviewers on the Reviewer List.

Concerning security baseline implications on existing analysis especially the risk of introducing insecurities to TLS in ‘normal’ use:

Reviewers were in general agreement that technical use of PSK, according to 8773, did not introduce concerns in undermining the current security achieved by TLS. I.e., introduction of the changes (ignoring the intent and the claimed security guarantees of 8773) do not seem to present security issues for TLS.

* The computational analysis seems fairly trivial. It will require some minor adaptions to existing models

* Effects of computational modeling with a quantum oracle are unclear.

# The fact that this extension does not affect how server authentication is achieved in a pre-quantum setting, seems convincing.

* It likely does not break anything from prior Tamarin analysis because that already assumes that the KDF is a dual-PRF, so it seems fairly straightforward to show that it maintains the same security properties.

# [It is like that the existing] analysis would carry over in an accordingly revised model combining PSKs and long-term signing keys, and asking for some hybrid guarantees from PSK+(EC)DHE. Now, such model change is cumbersome, but I wouldn't expect any surprises on that end.

Concerning claims in 8773 on security (ordering of quotes on authenticity roughly before quotes on confidentiality)

Reviewers were in general agreement about concerns on the security claims in the draft and what it achieves. This is particularly true about authentication claims but also applies to harvest-now-decrypt-later claims and provenance and access risks from the PSK. Since quantum resilience claims rest heavily on the PSK, how the PSK is generated, stored, and transferred (if relevant), are core to any claims of security that can be made for a quantum adversary setting. As a trivial case, if a traditional TLS (or other protocol) handshake is used to establish a session from which a PSK is derived, and that PSK is then later used with 8773, security claims for quantum resilience would be undermined.

# Imagine that the adversary has access to a quantum computer. Then, certificate authentication with classic algorithms is not viable anymore. Since the draft seems to aim hardening against quantum attackers without switching to PQ algorithms, it is currently not clear to me what kind of security properties are to be expected of the server authentication. The knowledge of PSK could clearly confer some type of authentication, and it seems a reasonable thing to conclude that this is achievable based on the current analyses as it appears that by eliminating the Certificate messages the handshake looks similar to the TLS1.3-PSK handshake.

# [It is unclear how] use of PSK confers authentication status on the TLS 1.3 handshake. The draft is (more or less) clear that for the server's authentication status, this should be instead provided by the {Certificate, CertificateVerified, Finished} messages. However, the draft does not specify how the authentication status of the client is affected, if _no_ client certificate authentication is used.

* Client authentication is currently underspecified.

# The draft seemingly would like to not make authentication assumptions on the PSK (at least pre-quantum), so there are some changes necessary in the [computational] proof to rely on certificate authentication instead. It seems to me that these changes will mostly look like copy/pasting proof steps from the proofs for the full TLS 1.3 handshake, though there are also additional changes necessary to argue security against the "decrypt later" adversary (which might resemble the no-ECDH proof more).

* it invalidates (almost) all the Tamarin proofs largely due to the changes in reasoning of security properties about the key schedule. This especially an issue for authentication.

# The new property that I think needs proving is the compound authentication property. Although not formally specified, the introduction suggests that the two methods of authentication are mutually exclusive, and goes on to talk about quantum computers breaking ECDH and ECDSA. I take this to mean that that if the classical asymmetric portions are broken then authentication is ensured by the symmetric PSK. Formally I would say that a client completing the protocol ostensibly with the server, knows that either the attacker has broken both the classical asymmetric portions *and* the symmetric PSK, or that _both_ have been used honestly (and vice versa).
This implies that if either mechanism is secure then the other is honest. This is a fairly subtle property to prove, and, and at least to me, it's not at all obvious that the property holds.

# The only thing where I don't know immediately [is] what precise guarantee one gets [since] PSKs can be shared among groups, and so authentication still depends on the signatures, but when a quantum computer arrives, everyone in the group could read other group members' communication. That sounds quite messy to model, but again, I wouldn't expect much surprise in the security guarantees one gets.

# I have to say I found the editorial quality of the RFC a bit tough. Especially Section 7 / Security Considerations is a bit blurry at times. E.g., I would say the protocol aims for hybrid guarantees as long as either PSK or (EC)DHE is secure; the RFC seems to only mention (EC)DHE breaking down. But then again, a bad PSK essentially makes this protocol be standard (EC)DHE + signatures, so security is expected also for this direction.

# I am not convinced a full security analysis (e.g., adjusting the proofs from [1]) is necessarily going to find anything interesting. But at the same time, modelling the types of attack that this draft aims to protect against (and could do better to specify) is possibly non-trivial (e.g., it might involve mixing of steps from the full, PSK-only and PSK-ECDH proofs in [1]).

# it claims to achieve a fairly complex and difficult to reason about property that TLS has never been demonstrated to provide.

** Existing analysis states "the full Hello messages ensure that session stages with an authenticated peer share hold exchanged Diffie–Hellman shares originating from an honest partner session". It was reasonable to one reviewer that the existing analysis could more-or-less can be mapped to the HNDL scenario even without properly modelling an HDNL attacker, but that the "hold exchanged Diffie–Hellman shares originating from an honest partner session" is a potential problem point especially with a pending quantum attacker.*
(NB: This links back to entity authentication above.)

# The achieved confidentiality is probably the security property in which this draft differs the most from the existing analyses. That is not so much because of the new mechanism, but because the draft claims to provide hardening against harvest-now-decrypt-later attacks, which have not been modeled in any prior analysis, to my knowledge. So the question becomes, how much of this is covered by prior analyses. The sketch of the proof provided in the Security Considerations does not seem sufficient to tackle this problem.

Other Warnings:
There was confusion among the reviewers about the case of 0-RTT. One reviewer wrote that, "The extension rules out using 0-RTT early data, which likely helps avoid many headaches" while another provided the note below. This points to some ambiguity in 8773, as illustrated by different interpretations. Both interpretations, however, point to concern on potential insecurities in a 0-RTT case.

# I would be on the look-out for implementation errors: [e.g., by] using an external PSK that has been compromised by the attacker before the test session completes, could you downgrade the handshake and cause the server to switch from PSK+SIG to just PSK? Does the implementation allow the external PSK to encrypt 0RTT data?

# It would be better to make more explicit that this extension intends to force-enable ephemeral key exchange (instead of burying it in section 5.1).

# Another thing that should probably be agreed upon is whether the keys for OOB PSK and OOB PSK with certs are disjoint. Without taking a closer look I'm not sure the PSK binder properties exactly capture the difference between the client offering and the server

accepting and the client offering and the server not supporting the extension, but connecting as a standard OOB handshake.
The specific issue I'm worried about is a client and server using the same set of keys for both PSK with certs and PSKs without certs (say during some transition period).

Concrete recommendations provided by reviewers:
It is noted in the review that the draft is ambiguous on the source of authenticity. In the description, authenticity is based on certificates and signatures, but it later states, “If the external PSK is known to any party other than the client and the server, then the external PSK MUST NOT be the sole basis for authentication.” This implies that in other cases the PSK may be the sole basis of authentication. Better clarity on this point is recommended.

# Better specify the targeted confidentiality and authenticity properties

* Clarify the situation regarding assumed authentication properties from the PSK for scenarios that are not covered by certificate authentication (client authentication status, RSA-is-broken authentication status)

# Provide a better proof sketch that also considers (HNDL) confidentiality rather than focuses on authentication

Notable relevant references:

[1]: Benjamin Dowling, Marc Fischlin, Felix Günther, Douglas Stebila. A Cryptographic Analysis of the TLS 1.3 Handshake Protocol (2023) https://eprint.iacr.org/2020/1044/

Reviewer List:
Dr. Benjamin Dowling
Dr. Felix Günther
Dr. Thom Wiggers
Dr. Jonathan Hoyland