Transport Layer Security
Internet-Draft
Intended status: Informational
Expires: 8 January 2026

M. U. Sardar
TU Dresden

7 July 2025

Extensions to TLS FATT Process
draft-usama-tls-fatt-extension-00

Abstract

This document proposes a new "Formal Analysis Considerations" section where the authors provide a threat model, informal security goals, and a protocol diagram. This document applies only to non-trivial extensions of TLS, which require formal analysis.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://muhammad-usama-sardar.github.io/tls-fatt-extension/draft-usama-tls-fatt-extension.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-usama-tls-fatt-extension/.

Discussion of this document takes place on the Transport Layer Security Working Group mailing list (mailto:tls@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/tls/. Subscribe at https://www.ietf.org/mailman/listinfo/tls/.

Source for this draft and an issue tracker can be found at https://github.com/muhammad-usama-sardar/tls-fatt-extension.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 8 January 2026.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

While the TLS FATT process [TLS-FATT] marks a historic change in achieving high cryptographic assurances by tightly integrating formal methods in the working group process, the current FATT process has some practical limitations. Given a relatively smaller formal methods community, and a steep learning curve as well as very low consideration of usability in the existing formal analysis tools, this document proposes some solutions to make the FATT process sustainable.

Specifically, the TLS FATT process does not outline the division of responsibility between the authors and the one doing the formal analysis (the latter is hereafter referred to as the "verifier"). This document aims to fill this gap without putting an extensive burden on either party.

An argument is often presented by the authors that an Internet-Draft is written for the implementers. With the FATT process, this argument is no longer valid. This document outlines the corresponding changes in the way Internet-Drafts are typically written. For the Internet-Draft to be useful for the formal analysis, this document proposes a new "Formal Analysis Considerations" section containing three main items, namely:

* a threat model,

* informal security goals, and

* a protocol diagram (Section 2.1).

Each one of these is summarized in Section 3. Future versions of this draft will include concrete examples.

Responsibilities of the verifier are summarized in Section 4.

1.1. Motivation

A clear separation of resposibilities would help IRTF UFMRG to train the authors and verifiers separately to fulfill their own responsibilities.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.1. Protocol Diagram

In the context of this document, a protocol diagram specifies the proposed cryptographically-relevant changes compared to the standard TLS protocol [I-D.ietf-tls-rfc8446bis]. This is conceptually similar to the Protocol Model in [RFC4101]. However, while [RFC4101] only recommends diagrams, we consider diagrams to be essential.

2.2. Definition of Attack

Any ambiguity originating from the threat model, informal security goals, and a protocol diagram is to be considered as an attack. The authors are, therefore, encouraged to be as precise as possible.

3. Responsibilities of Authors

This document proposes a new "Formal Analysis Considerations" section where the authors provide the following three items:

3.1. Threat Model

A threat model outlines the assumptions and known weaknesses of the proposed protocol. The threat model could be the classical Dolev-Yao adversary. In addition, it could specify any keys (e.g., long-term keys or session keys) which are assumed to be compromised (i.e., available to the adversary).

3.2. Informal Security Goals

Knowing what you want is the first step toward achieving it. Hence, informal security goals such as integrity, authentication, freshness, etc. should be outlined in the Internet-Draft. If the informal security goals are not spelled out in the Internet-Draft, it is safe to assume that the goals are still unclear to the authors. In such a case, the Internet-Draft should not be considered as ready for adoption.

3.3. Protocol Diagram

A protocol diagram should clearly mention the initial knowledge of the protocol participants, e.g., which authentic public keys are known to the protocol participants at the start of the protocol. An example of a protocol diagram for [I-D.fossati-tls-attestation-08] is provided in Section 3 of [Meeting-122-TLS-Slides].

4. Responsibilities of Verifier

When the authors declare the version as ready for formal analysis, the verifier takes the above inputs, performs the formal analysis, and brings the results back to the authors and the working group. Based on the analysis, the verifier may propose updates to the "Formal Analysis Considerations" section, Security Considerations section or other sections of the Internet-Draft.

5. Security Considerations

The whole document is about improving security considerations.

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

7.2. Informative References

[I-D.fossati-tls-attestation-08] Tschofenig, H., Sheffer, Y., Howard, P., Mihalcea, I., Deshpande, Y., Niemi, A., and T. Fossati, "Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", Work in Progress, Internet-Draft, draft-fossati-tls-attestation-08, 21 October 2024, <https://datatracker.ietf.org/doc/html/draft-fossati-tls-attestation-08>.

[I-D.ietf-tls-rfc8446bis] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-rfc8446bis-12, 17 February 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-rfc8446bis-12>.

[Meeting-122-TLS-Slides] Sardar, M. U., Moustafa, M., and T. Aura, "Identity Crisis in Attested TLS for Confidential Computing", March 2025, <https://datatracker.ietf.org/meeting/122/materials/slides-122-tls-identity-crisis-00>.

[RFC4101] Rescorla, E. and IAB, "Writing Protocol Models", RFC 4101, DOI 10.17487/RFC4101, June 2005, <https://www.rfc-editor.org/rfc/rfc4101>.

[TLS-FATT] IETF TLS WG, "TLS FATT Process", June 2025,
<https://github.com/tlswg/tls-fatt>.

Author’s Address

Muhammad Usama Sardar
TU Dresden
Email: muhammad_usama.sardar@tu-dresden.de