Using TLS in Applications
Internet-Draft
Updates: 9325 (if approved)
Intended status: Best Current Practice
Expires: 16 October 2025
R. Salz
Akamai Technologies
N. Aviram
14 April 2025

New Protocols Using TLS Must Require TLS 1.3
draft-ietf-uta-require-tls13-12

Abstract

TLS 1.3 use is widespread, it has had comprehensive security proofs, and it improves both security and privacy over TLS 1.2. Therefore, new protocols that use TLS must require TLS 1.3. As DTLS 1.3 is not widely available or deployed, this prescription does not pertain to DTLS (in any DTLS version); it pertains to TLS only.

This document updates RFC9325 and discusses post-quantum cryptography and the security and privacy improvements over TLS 1.2 as a rationale for that update.

About This Document

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

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-uta-require-tls13/.

Discussion of this document takes place on the Using TLS in Applications Working Group mailing list (mailto:uta@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/uta/. Subscribe at https://www.ietf.org/mailman/listinfo/uta/.

Source for this draft and an issue tracker can be found at https://github.com/richsalz/draft-use-tls13.

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 16 October 2025.

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

This document specifies that, since TLS 1.3 use is widespread, new protocols that use TLS must require and assume its existence. It updates [RFC9325] as described in Section 5. As DTLS 1.3 is not widely available or deployed, this prescription does not pertain to DTLS (in any DTLS version); it pertains to TLS only.

TLS 1.3 [TLS13] is in widespread use and fixes most known deficiencies with TLS 1.2. Examples of this include encrypting more of the traffic so that it is not readable by outsiders and removing most cryptographic primitives now considered weak. Importantly, the protocol has had comprehensive security proofs and should provide excellent security without any additional configuration.

TLS 1.2 [TLS12] is in use and can be configured such that it provides good security properties. However, TLS 1.2 suffers from several deficiencies, as described in Section 6. Addressing them usually requires bespoke configuration.

This document updates RFC9325 and discusses post-quantum cryptography and fixed weaknesses in TLS 1.2 as a rationale for that update.

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.

3. Implications for post-quantum cryptography (PQC)

Cryptographically-relevant quantum computers (CRQC), once available, will have a huge impact on TLS traffic (see, e.g., Section 2 of [I-D.ietf-pquip-pqc-engineers]). To mitigate this, TLS applications will need to migrate to Post-Quantum Cryptography (PQC) [PQC]. Detailed considerations of when an application requires PQC or when a CRQC is a threat that an application need to protect against, are beyond the scope of this document.

For TLS it is important to note that the focus of these efforts within the TLS WG is TLS 1.3 or later, and that TLS 1.2 will not be supported (see [TLS12FROZEN]). This is one more reason for new protocols require TLS to default to TLS 1.3, where PQC is actively being standardized, as this gives new applications the option to use PQC.

4. TLS Use by Other Protocols and Applications

Any new protocol that uses TLS MUST specify as its default TLS 1.3. For example, QUIC [QUICTLS] requires TLS 1.3 and specifies that endpoints MUST terminate the connection if an older version is used.

If deployment considerations are a concern, the protocol MAY specify TLS 1.2 as an additional, non-default option. As a counter example, the Usage Profile for DNS over TLS [DNSTLS] specifies TLS 1.2 as the default, while also allowing TLS 1.3. For newer specifications that choose to support TLS 1.2, those preferences are to be reversed.

The initial TLS handshake allows a client to specify which versions of the TLS protocol it supports and the server is intended to pick the highest version that it also supports. This is known as the "TLS version negotiation," and protocol and negotiation details are discussed in [TLS13], Section 4.2.1 and [TLS12], Appendix E. Many TLS libraries provide a way for applications to specify the range of versions they want, including an open interval where only the lowest or highest version is specified.

If the application is using a TLS implementation that supports this, and if it knows that the TLS implementation will use the highest version supported, then clients SHOULD specify just the minimum version they want. This MUST be TLS 1.3 or TLS 1.2, depending on the circumstances described in the above paragraphs.

5. Changes to RFC 9325

[RFC9325] provides recommendations for ensuring the security of deployed services that use TLS and, unlike this document, DTLS as well. At the time it was published, it described availability of TLS 1.3 as "widely available." The transition and adoption mentioned in that document has grown, and this document now makes two changes to the recommendations in [RFC9325], Section 3.1.1:

* That section says that TLS 1.3 SHOULD be supported; this document mandates that TLS 1.3 MUST be supported for new TLS-using protocols.

* That section says that TLS 1.2 MUST be supported; this document says that TLS 1.2 MAY be supported as described above.

Again, these changes only apply to TLS, and not DTLS.

6. Security Considerations

TLS 1.2 was specified with several cryptographic primitives and design choices that have, over time, become significantly weaker. The purpose of this section is to briefly survey several such prominent problems that have affected the protocol. It should be noted, however, that TLS 1.2 can be configured securely; it is merely much more difficult to configure it securely as opposed to using its modern successor, TLS 1.3. See [RFC9325] for a more thorough guide on the secure deployment of TLS 1.2.

Firstly, the TLS 1.2 protocol, without any extensions, is vulnerable to renegotiation attacks (see [RENEG1] and [RENEG2]) and the Triple Handshake attack (see [TRIPLESHAKE]). Broadly, these attacks exploit the protocol's support for renegotiation in order to inject a prefix chosen by the attacker into the plaintext stream. This is usually a devastating threat in practice, that allows e.g. obtaining secret cookies in a web setting. In light of the above problems, [RFC5746] specifies an extension that prevents this category of attacks. To securely deploy TLS 1.2, either renegotiation must be disabled entirely, or this extension must be used. Additionally, clients must not allow servers to renegotiate the certificate during a connection.

Secondly, the original key exchange methods specified for the protocol, namely RSA key exchange and finite field Diffie-Hellman, suffer from several weaknesses. Similarly, to securely deploy the protocol, most of these key exchange methods must be disabled. See [I-D.ietf-tls-deprecate-obsolete-kex] for details.

Thirdly, symmetric ciphers which were widely-used in the protocol, namely RC4 and CBC cipher suites, suffer from several weaknesses. RC4 suffers from exploitable biases in its key stream; see [RFC7465]. CBC cipher suites have been a source of vulnerabilities throughout the years. A straightforward implementation of these cipher suites inherently suffers from the Lucky13 timing attack [LUCKY13]. The first attempt to implement the cipher suites in constant time introduced an even more severe vulnerability [LUCKY13FIX]. There have been further similar vulnerabilities throughout the years exploiting CBC cipher suites; refer to, e.g., [CBCSCANNING] for an example and a survey of similar works.

In addition, TLS 1.2 was affected by several other attacks that TLS 1.3 is immune to: BEAST [BEAST], Logjam [WEAKDH], FREAK [FREAK], and SLOTH [SLOTH].

And finally, while application layer traffic is always encrypted, most of the handshake messages are not. Therefore, the privacy provided is suboptimal. This is a protocol issue that cannot be addressed by configuration.

7. IANA Considerations

This document makes no requests to IANA.

8. References

8.1. 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>.

[RFC9325] Sheffer, Y., Saint-Andre, P., and T. Fossati, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 9325, DOI 10.17487/RFC9325, November 2022, <https://www.rfc-editor.org/rfc/rfc9325>.

[TLS12] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/rfc/rfc5246>.

[TLS12FROZEN] Salz, R. and N. Aviram, "TLS 1.2 is in Feature Freeze", Work in Progress, Internet-Draft, draft-ietf-tls-tls12-frozen-08, 3 April 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-tls12-frozen-08>.

[TLS13] 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>.

8.2. Informative References

[BEAST] Duong, T. and J. Rizzo, "Here come the xor ninjas", n.d., <http://www.hpcc.ecs.soton.ac.uk/dan/talks/bullrun/Beast.pdf>.

[CBCSCANNING] Merget, R., Somorovsky, J., Aviram, N., Young, C., Fliegenschmidt, J., Schwenk, J., and Y. Shavitt, "Scalable Scanning and Automatic Classification of TLS Padding Oracle Vulnerabilities", n.d., <https://www.usenix.org/system/files/sec19-merget.pdf>.

[DNSTLS] Dickinson, S., Gillmor, D., and T. Reddy, "Usage Profiles for DNS over TLS and DNS over DTLS", RFC 8310, DOI 10.17487/RFC8310, March 2018, <https://www.rfc-editor.org/rfc/rfc8310>.

[FREAK] Beurdouche, B., Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Kohlweiss, M., Pironti, A., Strub, P.-Y., and J. K. Zinzindohoue, "A messy state of the union: Taming the composite state machines of TLS", n.d., <https://inria.hal.science/hal-01114250/file/messy-state-of-the-union-oakland15.pdf>.

[I-D.ietf-pquip-pqc-engineers] Banerjee, A., Reddy.K, T., Schoinianakis, D., Hollebeek, T., and M. Ounsworth, "Post-Quantum Cryptography for Engineers", Work in Progress, Internet-Draft, draft-ietf-pquip-pqc-engineers-09, 13 February 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-engineers-09>.

[I-D.ietf-tls-deprecate-obsolete-kex] Bartle, C. and N. Aviram, "Deprecating Obsolete Key Exchange Methods in TLS 1.2", Work in Progress, Internet-Draft, draft-ietf-tls-deprecate-obsolete-kex-05, 3 September 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-deprecate-obsolete-kex-05>.

[LUCKY13] Al Fardan, N. J. and K. G. Paterson, "Lucky Thirteen: Breaking the TLS and DTLS record protocols", n.d., <http://www.isg.rhul.ac.uk/tls/TLStiming.pdf>.

[LUCKY13FIX] Somorovsky, J., "Systematic fuzzing and testing of TLS libraries", n.d., <https://nds.rub.de/media/nds/veroeffentlichungen/2016/10/19/tls-attacker-ccs16.pdf>.

[PQC] "What Is Post-Quantum Cryptography?", August 2024, <https://www.nist.gov/cybersecurity/what-post-quantum-cryptography>.

[QUICTLS] Thomson, M., Ed. and S. Turner, Ed., "Using TLS to Secure QUIC", RFC 9001, DOI 10.17487/RFC9001, May 2021, <https://www.rfc-editor.org/rfc/rfc9001>.

[RENEG1] Rescorla, E., "Understanding the TLS Renegotiation Attack", n.d., <https://web.archive.org/web/20091231034700/http://www.educatedguesswork.org/2009/11/understanding_the_tls_renegoti.html>.

[RENEG2] Ray, M., "Authentication Gap in TLS Renegotiation", n.d., <https://web.archive.org/web/20091228061844/http://extendedsubset.com/?p=8>.

[RFC5746] Rescorla, E., Ray, M., Dispensa, S., and N. Oskov, "Transport Layer Security (TLS) Renegotiation Indication Extension", RFC 5746, DOI 10.17487/RFC5746, February 2010, <https://www.rfc-editor.org/rfc/rfc5746>.

[RFC7465] Popov, A., "Prohibiting RC4 Cipher Suites", RFC 7465, DOI 10.17487/RFC7465, February 2015, <https://www.rfc-editor.org/rfc/rfc7465>.

[SLOTH] Bhargavan, K. and G. Leurent, "Transcript collision attacks: Breaking authentication in TLS, IKE, and SSH", n.d., <https://inria.hal.science/hal-01244855/file/SLOTH_NDSS16.pdf>.

[TRIPLESHAKE] "Triple Handshakes Considered Harmful Breaking and Fixing Authentication over TLS", n.d., <https://mitls.org/pages/attacks/3SHAKE>.

[WEAKDH] Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J. A., Heninger, N., Springall, D., Thomテδゥ, E., Valenta, L., and B. VanderSloot, "Imperfect forward secrecy: How Diffie-Hellman fails in practice", n.d., <https://dl.acm.org/doi/pdf/10.1145/2810103.2813707>.

Authors’ Addresses

Rich Salz
Akamai Technologies
Email: rsalz@akamai.com

Nimrod Aviram
Email: nimrod.aviram@gmail.com