Stream:	Internet Engineering Task Force (IETF)
RFC:	9852
BCP:	195
Updates:	9325
Category:	Best Current Practice
Published:	January 2026
ISSN:	2070-1721
Authors:	R. Salz	N. Aviram
---	---	---
	Akamai Technologies	

RFC 9852
New Protocols Using TLS Must Require TLS 1.3

Abstract

TLS 1.3 is widely used, has had comprehensive security proofs, and improves both security and privacy deficiencies in 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 RFC 9325. It discusses post-quantum cryptography and the security and privacy improvements in TLS 1.3 as the rationale for the update.

Status of This Memo

This memo documents an Internet Best Current Practice.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on BCPs is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9852.

Copyright Notice

Table of Contents

1. Introduction

This document specifies that new protocols that use TLS must assume that TLS 1.3 is available and require its use. 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]. It discusses post-quantum cryptography and the security and privacy improvements in TLS 1.3 as the rationale for the update. See Section 5.

2. Conventions

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 (CRQCs), once available, will have a huge impact on TLS traffic (see, e.g., Section 3 of [PQC-FOR-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 needs to protect against are beyond the scope of this document.

It is important to note that the TLS Working Group is focusing its efforts on TLS 1.3 or later; TLS 1.2 will not be supported (see [TLS12FROZEN]). This is one more reason for new protocols to 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 TLS 1.3 as its default. 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 TLS it supports, and the server is intended to pick the highest version that it also supports. This is known as "TLS version negotiation"; protocol and negotiation details are discussed in Section 4.2.1 of [TLS13] and Appendix E of [TLS12]. 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 TLS version negotiation 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. [RFC9325] describes TLS 1.3 as "widely available", and the transition to TLS 1.3 has further increased since publication of that document. This document thus makes two changes to the recommendations in Section 3.1.1 of [RFC9325]:

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

First, without any extensions, TLS 1.2 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 (e.g., it allows an attacker to obtain 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.

Second, the original key exchange methods specified for TLS 1.2, namely RSA key exchange and finite field Diffie-Hellman, suffer from several weaknesses. To securely deploy the protocol, most of these key exchange methods must be disabled. See [KEY-EXCHANGE] for details.

Third, symmetric ciphers that are widely used in TLS 1.2, namely RC4 and Cipher Block Chaining (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]. Refer to [CBCSCANNING] for another example of a vulnerability with CBC cipher suites 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].

Finally, while application-layer traffic in TLS 1.2 is always encrypted, most of the content of the handshake messages is not. Therefore, the privacy provided is suboptimal. This is a protocol issue that cannot be addressed by configuration.

7. IANA Considerations

This document has no IANA actions.

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/info/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/info/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/info/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/info/rfc5246>.

[TLS12FROZEN] Salz, R. and N. Aviram, "TLS 1.2 is in Feature Freeze", RFC 9851, DOI 10.17487/RFC9851, January 2026, <https://www.rfc-editor.org/info/rfc9851>.

[TLS13] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 9846, DOI 10.17487/RFC9846, January 2026, <https://www.rfc-editor.org/info/rfc9846>.

8.2. Informative References

[BEAST] Duong, T. and J. Rizzo, "Here Come the XOR Ninjas", May 2011, <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", 28th USENIX Security Symposium (USENIX Security 19), August 2019, <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/info/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", IEEE Symposium on Security & Privacy 2015, HAL ID: hal-01114250, May 2015, <https://inria.hal.science/hal-01114250/file/messy-state-of-the-union-oakland15.pdf>.

[KEY-EXCHANGE] Aviram, N., "Deprecating Obsolete Key Exchange Methods in (D)TLS 1.2", Work in Progress, Internet-Draft, draft-ietf-tls-deprecate-obsolete-kex-07, 13 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-deprecate-obsolete-kex-07>.

[LUCKY13] Al Fardan, N. J. and K. G. Paterson, "Lucky Thirteen: Breaking the TLS and DTLS record protocols", February 2013, <http://www.isg.rhul.ac.uk/tls/TLStiming.pdf>.

[LUCKY13FIX] Somorovsky, J., "Systematic Fuzzing and Testing of TLS Libraries", CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 1492-1504, DOI 10.1145/2976749.2978411, October 2016, <https://nds.rub.de/media/nds/veroeffentlichungen/2016/10/19/tls-attacker-ccs16.pdf>.

[PQC] NIST, "What Is Post-Quantum Cryptography?", June 2025, <https://www.nist.gov/cybersecurity/what-post-quantum-cryptography>.

[PQC-FOR-ENGINEERS] Banerjee, A., Reddy, T., Schoinianakis, D., Hollebeek, T., and M. Ounsworth, "Post-Quantum Cryptography for Engineers", Work in Progress, Internet-Draft, draft-ietf-pquip-pqc-engineers-14, 25 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-engineers-14>.

[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/info/rfc9001>.

[RENEG1] Rescorla, E., "Understanding the TLS Renegotiation Attack", Wayback Machine archive, 5 November 2009, <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", Wayback Machine archive, <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/info/rfc5746>.

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

[SLOTH] Bhargavan, K. and G. Leurent, "Transcript Collision Attacks: Breaking Authentication in TLS, IKE, and SSH", Network and Distributed System Security Symposium - NDSS 2016, DOI 10.14722/ndss.2016.23418, HAL ID: hal-01244855, February 2016, <https://inria.hal.science/hal-01244855/file/SLOTH_NDSS16.pdf>.

[TRIPLESHAKE] "Triple Handshakes Considered Harmful: Breaking and Fixing Authentication over TLS", Wayback Machine archive, <https://web.archive.org/web/20250804151857/https://mitls.org/pages/attacks/3SHAKE>.

[WEAKDH] Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J. A., Heninger, N., Springall, D., Thome, E., Valenta, L., VanderSloot, B., Wustrow, E., Zanella-Beguelin, S., and P. Zimmerman, "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice", CCS '15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 5-17, DOI 10.1145/2810103.2813707, October 2015, <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