Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 22, 2021

J. Preuss Mattsson
Ericsson

November 18, 2020

Key Exchange Without Forward Secrecy is Not Recommended
draft-mattsson-tls-psk-ke-dont-dont-dont-00

Abstract

Key exchange without forward secrecy enables passive monitoring [RFC7258]. Massive pervasive monitoring attacks relying on key exchange without forward secrecy has been reported [I-D.ietf-emu-aka-pfs]. If key exchange without Diffe-Hellan is used, compromise of the long-term authenticatation key enables a passive attacker to compromise past and future sessions. All TLS 1.2 cipher suites without forward secrecy has been marked as NOT RECOMMENDED [RFC8447], and static RSA has been forbidden in TLS 1.3 [RFC8446]. psk_ke does not provide forward secrecy and is NOT RECOMMENDED. This document sets the IANA registration of psk_ke to NOT RECOMMENDED.

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 May 22, 2021.

Table of Contents

1. Terminology

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. IANA Considerations

IANA is requested to update the PskKeyExchangeMode registry under the Transport Layer Security (TLS) Parameters heading. For psk_ke the "Recommended" value has been set to "N".

3. References

3.1. 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>.

3.2. Informative References

[I-D.ietf-emu-aka-pfs]
Arkko, J., Norrman, K., and V. Torvinen, "Perfect-Forward Secrecy for the Extensible Authentication Protocol Method for Authentication and Key Agreement (EAP-AKA' PFS)", draft-ietf-emu-aka-pfs-05 (work in progress), October 2020.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/info/rfc7258>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC8447] Salowey, J. and S. Turner, "IANA Registry Updates for TLS and DTLS", RFC 8447, DOI 10.17487/RFC8447, August 2018, <https://www.rfc-editor.org/info/rfc8447>.

Acknowledgments

The authors want to thank Ari Keraenen for their valuable comments and feedback.

Author's Address

John Preuss Mattsson
Ericsson

Email: john.mattsson@ericsson.com