Network Working Group
Internet-Draft
Intended status: Informational
Expires: November 19, 2021

J. Preuss Mattsson
Ericsson

May 18, 2021

Key Exchange Without Forward Secrecy is NOT RECOMMENDED
draft-mattsson-tls-psk-ke-dont-dont-dont-01

Abstract

Key exchange without forward secrecy enables passive monitoring. Massive pervasive monitoring attacks relying on key exchange without forward secrecy has been reported, and many more have likely happened without ever being reported. If key exchange without Diffie-Hellman is used, access to the long-term authentication keys enables a passive attacker to compromise past and future sessions. Entities can get access to long-term key material in different ways: physical attacks, hacking, social engineering attacks, espionage, or by simply demanding access to keying material with or without a court order. 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 November 19, 2021.

Table of Contents

1. Introduction

Key exchange without forward secrecy enables passive monitoring [RFC7258]. Massive pervasive monitoring attacks relying on key exchange without forward secrecy has been reported [Heist] [I-D.ietf-emu-aka-pfs], and many more have likely happened without ever being reported. If key exchange without Diffie-Hellman is used, access to the long-term authentication keys enables a passive attacker to compromise past and future sessions. Entities can get access to long-term key material in different ways: physical attacks, hacking, social engineering attacks, espionage, or by simply demanding access to keying material with or without a court order.

All TLS 1.2 [RFC5246] cipher suites without forward secrecy has been marked as NOT RECOMMENDED [RFC8447], and static RSA has been forbidden in TLS 1.3 [RFC8446]. A large number of TLS profiles forbid use of key exchange without Diffie-Hellman for TLS 1.2 [RFC7540], [ANSSI], [TS3GPP].

- ANSSI states that for all versions of TLS: "The perfect forward secrecy property must be ensured."

- 3GPP based their general TLS 1.2 profile on [RFC7540] states: "Only cipher suites with AEAD (e.g. GCM) and PFS (e.g. ECDHE, DHE) shall be supported.

In addition to the very serious weaknesses of not providing protection against key leakage and enabling passive monitoring [RFC7258], psk_ke has other significant security problems. As stated in [RFC8446], psk_ke does not fulfill one of the fundamental TLS 1.3

security properties, namely "Forward secret with respect to long-term keys". When the PSK is a group key, which is now formally allowed in TLS 1.3 [I-D.ietf-tls-external-psk-guidance], psk_ke fails yet another one of the fundamental TLS 1.3 security properties, namely "Secrecy of the session keys" [Akhmetzyanova19] [I-D.ietf-tls-external-psk-guidance].

Together with ffdhe, and rsa_pkcs1, psk_ke is one of the bad apples in the TLS 1.3 fruit basket. Organizations like BSI [BSI] has already produced recommendations regarding TLS 1.3.

- BSI states regarding psk_ke that it "This mode should only be used in special applications after consultation of an expert." and has set a deadline of 2026 when psk_ke should not be used at all anymore.

Unfortunately psk_ke is marked as "Recommended" in the IANA PskKeyExchangeMode registry. This may weaken security in deployments following the "Recommended" column. Introducing TLS 1.3 in 3GPP had the unfortunate and surprising effect of drastically lowering the minimum security when TLS is used with PSK authentication. Some companies in 3GPP has been unwilling to disrecommend psk_ke as IETF has so clearly marked it as "Recommended".

PSK authentication has yet another big inherent weakness as it does not provide "Protection of endpoint identities". It could be argued that PSK authentication should be not recommended solely based on this significant privacy weakness.

This document updates the PskKeyExchangeMode registry under the Transport Layer Security (TLS) Parameters heading. For psk_ke the "Recommended" value has been set to "N".

Editor's note: The current IANA action is based on the present very limited single column in the IANA TLS registries. If more granular classifications were possible in the future, it would likely make

sense to difference between different use cases where psk_ke might be useful such as very constrained IoT.

1.1. 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>.

[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>.

3.2. Informative References

[Akhmetzyanova19]
Akhmetzyanova, L., Alekseev, E., Smyshlyaeva, E., and A. Sokolov, "Continuing to reflect on TLS 1.3 with external PSK", April 2019, <https://eprint.iacr.org/2019/421.pdf>.

[ANSSI] Agence nationale de la securite des systemes d'information, ., "Security Recommendations for TLS", January 2017, <https://www.ssi.gouv.fr/uploads/2017/02/security-recommendations-for-tls_v1.1.pdf>.

[BSI] Bundesamt fuer Sicherheit in der Informationstechnik, ., "Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths Part 2 - Use of Transport Layer Security (TLS)", January 2021, <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-2.pdf>.

[Heist] The Intercept, ., "How Spies Stole the Keys to the Encryption Castle", February 2015, <https://theintercept.com/2015/02/19/great-sim-heist/>.

[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.

[I-D.ietf-tls-external-psk-guidance]
Housley, R., Hoyland, J., Sethi, M., and C. A. Wood, "Guidance for External PSK Usage in TLS", draft-ietf-tls-external-psk-guidance-02 (work in progress), February 2021.

[RFC5246] 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>.

[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>.

[RFC7540] Belshe, M., Peon, R., and M. Thomson, Ed., "Hypertext Transfer Protocol Version 2 (HTTP/2)", RFC 7540, DOI 10.17487/RFC7540, May 2015, <https://www.rfc-editor.org/info/rfc7540>.

[TS3GPP] 3GPP, ., "TS 33.210 Network Domain Security (NDS); IP network layer security", July 2020, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2279>.

Acknowledgements

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

Author's Address

John Preuss Mattsson
Ericsson AB
SE-164 80 Stockholm
Sweden

Email: john.mattsson@ericsson.com