Internet Engineering Task Force (IETF)
Request for Comments: 7465
Updates: 5246, 4346, 2246
Category: Standards Track
ISSN: 2070-1721

A. Popov
Microsoft Corp.

February 2015

Prohibiting RC4 Cipher Suites

Abstract

This document requires that Transport Layer Security (TLS) clients and servers never negotiate the use of RC4 cipher suites when they establish connections. This applies to all TLS versions. This document updates RFCs 5246, 4346, and 2246.

Status of This Memo

This is an Internet Standards Track document.

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 Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7465.

Table of Contents

1. Introduction

RC4 is a stream cipher that is described in [SCH]; it is widely supported, and often preferred by TLS servers. However, RC4 has long been known to have a variety of cryptographic weaknesses, e.g., see [PAU], [MAN], and [FLU]. Recent cryptanalysis results [ALF] exploit biases in the RC4 keystream to recover repeatedly encrypted plaintexts.

These recent results are on the verge of becoming practically exploitable; currently, they require 2^26 sessions or 13x2^30 encryptions. As a result, RC4 can no longer be seen as providing a sufficient level of security for TLS sessions.

This document requires that TLS ([RFC5246] [RFC4346] [RFC2246]) clients and servers never negotiate the use of RC4 cipher suites.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Changes to TLS

Because of the RC4 deficiencies noted in Section 1, the following apply:

- TLS clients MUST NOT include RC4 cipher suites in the ClientHello message.
- TLS servers MUST NOT select an RC4 cipher suite when a TLS client sends such a cipher suite in the ClientHello message.

- If the TLS client only offers RC4 cipher suites, the TLS server MUST terminate the handshake. The TLS server MAY send the insufficient_security fatal alert in this case.

Appendix A lists the RC4 cipher suites defined for TLS.

3. Security Considerations

This document helps maintain the security guarantees of the TLS protocol by prohibiting the use of the RC4-based cipher suites (listed in Appendix A), which do not provide a sufficiently high level of security.

4. References

4.1. Normative References

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

[RFC2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999, <http://www.rfc-editor.org/info/rfc2246>.

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006, <http://www.rfc-editor.org/info/rfc4346>.

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

4.2. Informative References

[ALF] AlFardan, N., Bernstein, D., Paterson, K., Poettering, B., and J. Schuldt, "On the Security of RC4 in TLS and WPA", USENIX Security Symposium, July 2013, <https://www.usenix.org/conference/usenixsecurity13/security-rc4-tls>.

[FLU] Fluhrer, S., Mantin, I., and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", Selected Areas of Cryptography: SAC 2001, Lecture Notes in Computer Science Vol. 2259, pp 1-24, 2001.

[MAN] Mantin, I. and A. Shamir, "A Practical Attack on Broadcast RC4", Fast Software Encryption: FSE 2001, Lecture Notes in Computer Science Vol. 2355, pp 152-164, 2002.

[PAU] Paul, G. and S. Maitra, "Permutation after RC4 Key Scheduling Reveals the Secret Key", Selected Areas of Cryptography: SAC 2007, Lecture Notes on Computer Science, Vol. 4876, pp 360-337, 2007.

[SCH] Schneier, B., "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2nd Edition, 1996.

Appendix A. RC4 Cipher Suites

The following cipher suites defined for TLS use RC4:

- TLS_RSA_EXPORT_WITH_RC4_40_MD5
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA
- TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
- TLS_DH_anon_WITH_RC4_128_MD5
- TLS_KRB5_WITH_RC4_128_SHA
- TLS_KRB5_WITH_RC4_128_MD5
- TLS_KRB5_EXPORT_WITH_RC4_40_SHA
- TLS_KRB5_EXPORT_WITH_RC4_40_MD5
- TLS_PSK_WITH_RC4_128_SHA
- TLS_DHE_PSK_WITH_RC4_128_SHA
- TLS_RSA_PSK_WITH_RC4_128_SHA
- TLS_ECDH_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDH_RSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_ECDH_anon_WITH_RC4_128_SHA
- TLS_ECDHE_PSK_WITH_RC4_128_SHA

Acknowledgements

This document was inspired by discussions with Magnus Nystrom, Eric Rescorla, Joseph Salowey, Yaron Sheffer, Nagendra Modadugu, and others on the TLS mailing list.

Author's Address

Andrei Popov
Microsoft Corp.
One Microsoft Way
Redmond, WA 98052
USA

EMail: andreipo@microsoft.com