Internet Engineering Task Force
Internet-Draft
Updates: 5246,4346,2246 (if approved)
Intended status: Standards Track
Expires: October 13, 2014

A. Popov
Microsoft Corp.

April 11, 2014

Prohibiting RC4 Cipher Suites
draft-popov-tls-prohibiting-rc4-02

Abstract

This document requires that Transport Layer Security (TLS) clients and servers never negotiate the use of RC4 cipher suites when they establish connections.

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 http://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 October 13, 2014.

Copyright Notice

Table of Contents

1. Introduction

RC4 is a stream cipher described in [SCH], which is widely supported, and often preferred, by TLS servers. However, RC4 has long been known to have a variety of cryptographic weaknesses, e.g. [PAU], [MAN], [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 deficiencies noted in Section 1:

- 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.

- o 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. 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.

4. IANA Considerations

This memo includes no request to IANA.

5. 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.

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

6.2. 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.", 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 in Cryptography, pp. 1-24", 2001.

[MAN] Mantin, I. and A. Shamir, "A Practical Attack on Broadcast RC4. FSE, pp. 152-164.", 2001.

[PAU] Paul, G. and S. Maitra, "Permutation after RC4 Key Scheduling Reveals the Secret Key. In Proceedings of the 14th Workshop on Selected Areas in Cryptography (SAC), pp. 360-377, vol. 4876, LNCS, Springer.", 2007.

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

Appendix A. RC4 Cipher Suites

The following cipher suites defined for TLS use RC4:

- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA
- TLS_DH_anon_WITH_RC4_128_MD5
- TLS_RSA_EXPORT_WITH_RC4_40_MD5
- TLS_DH_anon_EXPORT_WITH_RC4_40_MD5

Author’s Address

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

Email: andreipo@microsoft.com