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.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
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 $13 \times 2^{30}$ 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


4.2. Informative References


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