Network Working Group
Internet Draft
Updates: 5246, 4346, 2246 (once approved)
Intended Status: Standards Track
Expires: June 16, 2011

S. Turner
IECA
T. Polk
NIST

December 16, 2010

Prohibiting SSL Version 2.0
draft-ietf-tls-ssl2-must-not-04.txt

Abstract

This document requires that when TLS clients and servers establish connections that they never negotiate the use of Secure Sockets Layer (SSL) version 2.0. This document updates the backward compatibility sections found in the Transport Security Layer (TLS).

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79. This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on May 16, 2009.

1. Introduction

Many protocols specified in the IETF rely on Transport Layer Security (TLS) [TLS1.0][TLS1.1][TLS1.2] for security services. This is a good thing, but some TLS clients and servers also support negotiating the use of Secure Sockets Layer (SSL) version 2.0 [SSL2]; however, this version does not provide a sufficiently high level of security. SSL version 2.0 has known deficiencies. This document describes those deficiencies, and it requires TLS clients and servers never negotiate the use of SSL version 2.0.

TLS 1.1 [RFC4346] and later in TLS 1.2 [RFC5246] explicitly warned implementers that the "ability to send version 2.0 CLIENT-HELLO messages will be phased out with all due haste." This document accomplishes this by updating the backward compatibility sections found in TLS [TLS1.0][TLS1.1][TLS1.2].

1.1. Requirements 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 [RFC2119].

2. SSL 2.0 Deficiencies

SSL version 2.0 [SSL2] deficiencies include:

- Message authentication uses MD5 [MD5]. Most security-aware users have already moved away from any use of MD5 [I-D.turner-md5-seccon-update].

- Handshake messages are not protected. This permits a man-in-the-middle to trick the client into picking a weaker cipher suite than they would normally choose.

- Message integrity and message encryption use the same key, which is a problem if the client and server negotiate a weak encryption algorithm.

- Sessions can be easily terminated. A man-in-the-middle can easily insert a TCP FIN to close the session and the peer is unable to determine whether or not it was a legitimate end of the session.

3. Changes to TLS

Because of the deficiencies noted in the previous section:

- TLS clients MUST NOT send the SSL version 2.0 compatible CLIENT-HELLO message format. Clients MUST NOT send any client hello message which specifies a protocol version less than { 0x03, 0x00 }. As previously stated by the definitions of all previous versions of TLS, the client SHOULD specify the highest protocol version it supports.

- TLS servers MAY continue to accept CLIENT-HELLO messages in the version 2 CLIENT-HELLO format as specified in TLS 1.2 [RFC5246] Appendix E.2. Note that this does not contradict the prohibition against actually negotiating the use of SSL 2.0.

  TLS Servers MUST NOT reply with a SSL 2.0 SERVER-HELLO with a protocol version which is less than { 0x03, 0x00 } and instead MUST abort the connection, i.e., when the highest protocol version offered by the client is { 0x02, 0x00 } the TLS connection will be refused.

Note that the number of servers that support this above-mentioned "MAY accept" implementation option is declining, and the SSL 2.0 CLIENT-HELLO precludes the use of TLS protocol enhancements that require TLS extensions. TLS extensions can only be sent as part of an (Extended) ClientHello handshake message.

4. IANA Considerations

None.

5. Security Considerations

This entire document is about security considerations.

6. Acknowledgements

The idea for this document was inspired by discussions between Peter Saint Andre, Simon Josefsson, and others on the XMPP mailing list.

We would also like to thank Michael D'Errico, Paul Hoffman, Nikos Mavrogiannopoulos, Tom Petch, Yngve Pettersen, Marsh Ray, Martin Rex, Yaron Sheffer, and Glen Zorn for their reviews and comments.

7. References

7.1. Normative References

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

[TLS1.0] Dierks, T., and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[TLS1.1] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[TLS1.2] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

7.2. Informative References

[MD5] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[SSL2] Hickman, Kipp, "The SSL Protocol", Netscape Communications Corp., Feb 9, 1995.

[I-D.turner-md5-seccon-update] Turner, S., and L. Chen, "Updated Security Considerations for the MD5 Message-Digest Algorithm", draft-turner-md5-seccon-update, work-in-progress.

Authors' Addresses

Sean Turner
IECA, Inc.
3057 Nutley Street, Suite 106
Fairfax, VA 22031
USA

EMail: turners@ieca.com

Tim Polk
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8930
Gaithersburg, MD 20899-8930
USA

EMail: tim.polk@nist.gov