

Network Working Group  
Internet Draft  
Updates: [5246](#) (once approved)  
Intended Status: Standards Track  
Expires: February 23, 2011

S. Turner  
IECA  
Tim Polk  
NIST  
August 23, 2010

Prohibiting SSL Version 2.0  
draft-ietf-tls-ssl2-must-not-00.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) Protocol, [RFC 5246](#).

## 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/lid-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 February 23, 2009.

## Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

Internet-Draft

Prohibiting SSL 2.0

August 2010

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

Many protocols specified in the IETF rely on Transport Layer Security (TLS) [[TLS](#)] for security services. This is a good thing, but some TLS clients and servers also support negotiating the use of SSL version 2.0 [[SSL2](#)]; however, this version does not provide the expected 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.

This document updates the backward compatibility sections found in the Transport Security Layer (TLS) Protocol [[TLS](#)] and earlier versions.

### 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

SSL version 2.0 [[SSL2](#)] deficiencies include:

- o Message authentication uses MD5 [[MD5](#)]. Most security-aware users have already moved away from any of MD5 [[I-D.turner-md5-secon-update](#)].
- o 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.

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

- o 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 sections, TLS implementations MUST NOT support SSL 2.0. The specific changes to [\[TLS\]](#), including earlier versions, are as follows:

- o TLS clients MUST NOT use SSL 2.0 ClientHello messages.
- o TLS servers MUST NOT accept SSL 2.0 ClientHello messages.

### [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 Paul Hoffman, Yaron Sheffer, and Nikos Mavrogiannopoulos, Yngve Pettersen, Marsh Ray, and Martin Rex for reviews and comments on earlier versions of this document.

### [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.
- [TLS] 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.

Turner and Polk Expires February 23, 2011 [Page 3]

---

Internet-Draft Prohibiting SSL 2.0 August 2010

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

### Authors' Addresses

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

E-Mail: [turners@ieca.com](mailto:turners@ieca.com)

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

E-Mail: [tim.polk@nist.gov](mailto:tim.polk@nist.gov)

Turner and Polk

Expires February 23, 2011

[Page 4]