        Transport Layer Security Protocol Compression Methods
                  draft-ietf-tls-compression-00.txt

Status of this Memo

   This document is an Internet-Draft and is in full conformance with
   all provisions of Section 10 of RFC2026.

   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 March 6, 2003.

Copyright Notice

Abstract

   The Transport Layer Security (TLS) protocol (RFC 2246) includes
   features to negotiate selection of a lossless data compression method
   as part of the TLS Handshake Protocol and to then apply the algorithm
   associated with the selected method as part of the TLS Record
   Protocol. TLS defines one standard compression method,
   CompressionMethod.null, which specifies that data exchanged via the
   record protocol will not be compressed. This document describes
   additional compression methods associated with lossless data
   compression algorithms for use with TLS.

Conventions Used In This Document

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 RFC 2119 [1].

Table of Contents

1. Introduction

The Transport Layer Security (TLS) protocol (RFC 2246, [2]) includes
features to negotiate selection of a lossless data compression method
as part of the TLS Handshake Protocol and to then apply the algorithm
associated with the selected method as part of the TLS Record
Protocol. TLS defines one standard compression method,
CompressionMethod.null, which specifies that data exchanged via the
record protocol will not be compressed. While this single
compression method helps ensure that TLS implementations are
interoperable, the lack of additional standard compression methods
has limited the ability of implementers to develop interoperable
implementations that include data compression.

TLS is used extensively to secure client-server connections on the
World Wide Web. While these connections can often be characterized
as short-lived and exchanging relatively small amounts of data, TLS
is also being used in environments where connections can be long-
lived and the amount of data exchanged can extend into thousands or
millions of octets. XML [4], for example, is increasingly being used
as a data representation method on the Internet, and XML tends to be
verbose. Compression within TLS is one way to help reduce the
bandwidth and latency requirements associated with exchanging large
amounts of data while preserving the security services provided by
TLS.

This document describes additional compression methods associated
with lossless data compression algorithms for use with TLS.
Standardization of the compressed data formats and compression
algorithms associated with the compression methods is beyond the
scope of this document.

2. **Compression Methods**

   TLS [2] includes the following compression method structure in
   sections 6.1 and 7.4.1.2 and Appendix sections A.4.1 and A.6:

   enum { null(0), (255) } CompressionMethod;

   which allows for later specification of up to 256 different
   compression methods. This definition is updated to segregate the
   range of allowable values into three zones:

   1. Values from 0 (zero) through 63 decimal (0x3F) inclusive are
       reserved for future standardization efforts of the IETF TLS
       working group.

   2. Values from 64 decimal (0x40) through 192 decimal (0xC0) are
       reserved for assignment by the IANA for specifications developed
       outside the TLS working group. Assignments from this range of
       values MUST be made by the IANA and MUST be associated with a
       formal reference that describes the compression method.

   3. Values from 193 decimal (0xC1) through 255 decimal (0xFF) are
       reserved for private use.

   Additional information describing the role of the IANA in the
   allocation of compression method identifiers is described in Section
   5.

   In addition, this definition is updated to include assignment of
   three additional compression methods:

   enum { null(0), ZLIB(1), LZS(2), RLE(3), (255) } CompressionMethod;

   The ZLIB compression method is described in RFC 1950 [5]. The Lempel
   Zif Stac (LZS) compression method is described in ANSI publication
   X3-241 [6]. The Run Length Encoding (RLE) compression method is
   described in part 5 of the Digital Imaging and Communications in
   Medicine standard [7].

[3](#). **Intellectual Property Considerations**

   Many compression algorithms are subject to patent or other
   intellectual property rights claims. Implementers are encouraged to
   seek legal guidance to better understand the implications of
   developing implementations of the compression methods described in
   this document.

4. Internationalization Considerations

   The compression method identifiers specified in this document are
   machine-readable numbers. As such, issues of human
   internationalization and localization are not introduced.

5. **IANA Considerations**

   This document does not have a direct impact on the IANA, but it does
   define ranges of compression method values for future assignment.
   Values from the range reserved for future standardization efforts of
   the TLS working group MUST be assigned according to the "Standards
   Action" policy described in RFC 2434 [3]. Values from the range
   reserved for private use MUST be used according to the "Private Use"
   policy described in RFC 2434. Values from the general IANA pool MUST
   be assigned according to the "IETF Consensus" policy described in RFC
   2434.

[6](#). **Security Considerations**

   This document does not introduce any topics that alter the threat
   model addressed by TLS. However, data compression prior to
   encryption can potentially provide a security benefit in "flattening"
   the distribution of unencrypted octets (or increasing the unicity
   distance) by using fewer bits to represent common characters. In
   situations where the unencrypted octets represent human-readable
   text, reducing the predictability of text patterns can make it
   slightly more difficult to mount a successful attack on the encrypted
   octets.

[7](#). Acknowledgements

   The concepts described in this document were originally discussed on
   the IETF TLS working group mailing list in December, 2000. The
   author acknowledges the contributions to that discussion provided by
   Jeffrey Altman, Eric Rescorla, and Marc Van Heyningen.

Normative References

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

    [2]   Dierks, T., Allen, C., Treese, W., Karlton, P., Freier, A. and
          P. Kocher, "The TLS Protocol Version 1.0", RFC 2246, January
          1999.

    [3]   Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA
          Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

Informative References

    [4]   Bray, T., Paoli, J., Sperberg-McQueen, C. and E. Maler,
          "Extensible Markup Language (XML) 1.0 (2nd ed)", W3C REC-xml,
          October 2000, <http://www.w3.org/TR/REC-xml>.

    [5]   Deutsch, L. and J-L. Gailly, "ZLIB Compressed Data Format
          Specification version 3.3", RFC 1950, May 1996.

    [6]   American National Standards Institute, "Data Compression Method,
          Adaptive Coding with Sliding Window of Information Interchange",
          ANSI X3.241, 1994.

    [7]   National Electrical Manufacturers Association, "Digital Imaging
          and Communications in Medicine (DICOM) Part 5: Data Structures
          and Encoding", 2001, <http://medical.nema.org/dicom/2001/
          01_05PU.PDF>.

Author's Address

    Scott Hollenbeck
    VeriSign, Inc.
    21345 Ridgetop Circle
    Dulles, VA   20166-6503
    US

    EMail: shollenbeck@verisign.com