Network Working Group
Internet-Draft
Expires: May 5, 2014

A. Langley
Google Inc
Nov 2013

A TLS padding extension
draft-agl-tls-padding-02

Abstract

This memo describes the a TLS extension that can be used to pad ClientHello messages to a desired size.

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 May 5, 2014.

Table of Contents

1. Introduction 3
2. Requirements Notation 4
3. Padding Extension 5
4. Example usage 6
5. Security Considerations 7
6. IANA Considerations 8
7. Normative References 9
Author's Address 10

1. Introduction

Successive TLS [RFC5246] versions have added support for more cipher suites and, over time, more TLS extensions have been defined. This has caused the size of the TLS ClientHello to grow and the additional size has caused some implementation bugs to come to light. At least one of these implementation bugs can be ameliorated by making the ClientHello even larger.

This memo describes a TLS extension that can be used to pad a ClientHello to a desired size in order to avoid implementation bugs caused by certain ClientHello sizes.

2. Requirements Notation

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 [RFC2119].

3. Padding Extension

A new extension type (""padding(TBD)"") is defined and MAY be included by the client in its ClientHello message.

```
enum {
        padding(TBD), (65535)
} ExtensionType
```

The client MUST fill the padding extension completely with zero bytes, although the padding extension may be empty.

The server MUST NOT echo the extension.

4. Example usage

As an example, consider a client that wishes to avoid sending a ClientHello with a record size between 256 and 511 bytes (inclusive). This case is considered because at least one TLS implementation is known to hang the connection when such a ClientHello record is received.

After building a ClientHello as normal, the client can add four to the length (to account for the handshake protocol overhead) and test whether the resulting length falls into that range. If it does, a padding extension can be added in order to push the length to (at least) 512 bytes.

Note that if the original ClientHello size was between 505 and 508 bytes then, with the handshake overhead, the record would be between 509 and 511 bytes long. Since it's not possible for an extension to take less than four bytes of space, the additional padding would have to expand the ClientHello record past 512 bytes in these cases.

5. Security Considerations

The contents of the padding extension could be used as a side-channel. In order to prevent this, the contents are required to be all zeros, although the length of the extension can still be used as a much smaller side-channel. Servers MAY verify that the extension is either empty or contains only zero bytes, in order to enforce this.

6. IANA Considerations

IANA is requested to assign an extension value for the padding extension from its ExtensionType registry.

7. Normative References

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

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

Author's Address

Adam Langley
Google Inc

Email: agl@google.com