< draft-ietf-tsvwg-transport-encrypt-14.txt

TSVWG G. Fairhurst
Internet-Draft University of Aberdeen
Intended status: Informational C. Perkins
Expires: October 5, 2020 University of Glasgow
April 03, 2020

Considerations around Transport Header Confidentiality, Network Operations, and the Evolution of Internet Transport Protocols
draft-ietf-tsvwg-transport-encrypt-14

Abstract

To protect user data and privacy, Internet transport protocols have supported payload encryption and authentication for some time. Such encryption and authentication is now also starting to be applied to the transport protocol headers. This helps avoid transport protocol ossification by middleboxes, while also protecting metadata about the communication. Current operational practice in some networks inspect transport header information within the network, but this is no

skipping to change at *page 1, line 45*

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 https://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 October 5, 2020.

Copyright Notice

Copyright (c) 2020 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 (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents

skipping to change at *page 2, line 30*

Table of Contents

1. Introduction

Transport protocols have supported end-to-end encryption of payload data for many years. Examples include Transport Layer Security (TLS) over TCP [RFC8446], Datagram TLS (DTLS) over UDP [RFC6347], Secure RTP [RFC3711], and TCPcrypt [RFC8548] which permits opportunistic encryption of the TCP transport payload. Some of these also provide

skipping to change at *page 13, line 20*

Observable transport header information, together with information in the network header, has been used to identify flows and their connection state, together with the set of protocol options being used. Transport protocols, such as TCP and the Stream Control Transport Protocol (SCTP), specify a standard base header that includes sequence number information and other data. They also have the possibility to negotiate additional headers at connection setup, identified by an option number in the transport header.

In some uses, a low-numbered (well-known) transport port number can identify the protocol. However, port information alone is not sufficient to guarantee identification. Applications can use arbitrary ports, multiple sessions can be multiplexed on a single port, and ports can be re-used by subsequent sessions. UDP-based protocols often do not use well-known port numbers. Some flows can be identified by observing signalling protocol data (e.g., [RFC3261], [I-D.ietf-rtcweb-overview]) or through the use of magic numbers placed in the first byte(s) of the datagram payload [RFC7983].

draft-ietf-tsvwg-transport-encrypt-15.txt >

TSVWG G. Fairhurst
Internet-Draft University of Aberdeen
Intended status: Informational C. Perkins
Expires: October 8, 2020 University of Glasgow
April 06, 2020

Considerations around Transport Header Confidentiality, Network Operations, and the Evolution of Internet Transport Protocols
draft-ietf-tsvwg-transport-encrypt-15

Abstract

To protect user data and privacy, Internet transport protocols have supported payload encryption and authentication for some time. Such encryption and authentication is now also starting to be applied to the transport protocol headers. This helps avoid transport protocol ossification by middleboxes, while also protecting metadata about the communication. Current operational practice in some networks inspect transport header information within the network, but this is no

skipping to change at *page 1, line 45*

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 https://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 October 8, 2020.

Copyright Notice

Copyright (c) 2020 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 (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents

skipping to change at *page 2, line 30*

Table of Contents

1. Introduction

Transport protocols have supported end-to-end encryption of payload data for many years. Examples include Transport Layer Security (TLS) over TCP [RFC8446], Datagram TLS (DTLS) over UDP [RFC6347], Secure RTP [RFC3711], and TCPcrypt [RFC8548] which permits opportunistic encryption of the TCP transport payload. Some of these also provide

skipping to change at *page 13, line 20*

Observable transport header information, together with information in the network header, has been used to identify flows and their connection state, together with the set of protocol options being used. Transport protocols, such as TCP and the Stream Control Transport Protocol (SCTP), specify a standard base header that includes sequence number information and other data. They also have the possibility to negotiate additional headers at connection setup, identified by an option number in the transport header.

In some uses, an assigned transport port (e.g., 0..49151) can identify the protocol [RFC7605]. However, port information alone is not sufficient to guarantee identification. Applications can use arbitrary ports and do not need to use well-known port numbers. The use of a well-known port number is also not limited to the protocol for which the port is well known. Multiple sessions can also be multiplexed on a single port, and ports can be re-used by subsequent sessions.

Some flows can be identified by observing signalling protocol data (e.g., [RFC3261], [I-D.ietf-rtcweb-overview]) or through the use of magic numbers placed in the first byte(s) of the datagram payload [RFC7983].

When transport header information can not be observed, this removes information that could have been used to classify flows by passive observers along the path. More ambitious ways could be used to collect, estimate, or infer flow information, including heuristics based on the analysis of traffic patterns. For example, an operator that cannot access the Session Description Protocol (SDP) session descriptions to classify a flow as audio traffic, might instead use (possibly less-reliable) heuristics to infer that short UDP packets with regular spacing carry audio traffic. Operational practises

skipping to change at *page 29, line 39* / skipping to change at *page 29, line 47*

transport information observable by the network. Another approach is to choose to expose transport information through the use of network-layer extension headers. Both are examples of explicit signals that the information is intended to be used by network devices on the path [RFC8558].

Whatever the mechanism used to expose the information, a decision to only expose specific transport information, places the transport endpoint in control of what to expose or not to expose outside of the encrypted transport header. This decision can then be made independently of the transport protocol functionality. This provides opportunities to standardise the method and format used to expose this transport information. This can be done by exposing part of the transport header or as a network layer option/extension.

6.1. Exposing Transport Information in Extension Headers

At the network-layer, packets can carry optional headers (similar to Section 5) that may be used to explicitly expose transport header information to the on-path devices operating at the network layer (Section 3.1.3). For example, an endpoint that sends an IPv6 Hop-by-Hop option [RFC8200] can provide explicit transport layer information that can be observed and used by network devices on the path.

Network-layer optional headers explicitly indicate the information that is exposed, whereas use of exposed transport header information first requires an observer to identify the transport protocol and its format. See Section 3.1.1 for further discussion of transport protocol identification.

An arbitrary path can include one or more network devices that drop packets that include a specific header or option used for this purpose (see [RFC7872]). This could impact the proper functioning of the protocols using the path. Protocol methods can be designed to probe to discover whether the specific option(s) can be used along the current path, enabling use on arbitrary paths.

6.2. Common Exposed Transport Information

There are opportunities for multiple transport protocols to

skipping to change at *page 30, line 48* / skipping to change at *page 31, line 14*

evolution of transport-independent tools around a common observable header, and permit transport protocols to also evolve independently of this ossified header [RFC8558].

- On the other hand, protocols and implementations may not consistently expose external information that reflects the actual internal information used by the protocol itself. An endpoint/protocol could choose to expose transport header information to optimise the benefit it gets from the network [RFC8558]. The value of this information would be enhanced if the exposed information could be verified to match the internal state of the transport by observing the transport behaviour.

7. Implications of Protecting the Transport Headers

The choice of which transport header fields to expose and which to encrypt is a design decision for the transport protocol. Selective encryption requires trading conflicting goals of observability and network support, privacy, and risk of ossification, to decide what header fields to protect and which to make visible.

Security work typically employs a design technique that seeks to

skipping to change at *page 46, line 20* / skipping to change at *page 46, line 35*

Recommendations Regarding Active Queue Management", BCP 197, RFC 7567, DOI 10.17487/RFC7567, July 2015, <https://www.rfc-editor.org/info/rfc7567>.

[RFC7594] Eardley, P., Morton, A., Bagnulo, M., Burbridge, T., Aitken, P., and A. Akhter, "A Framework for Large-Scale Measurement of Broadband Performance (LMAP)", RFC 7594, DOI 10.17487/RFC7594, September 2015, <https://www.rfc-editor.org/info/rfc7594>.

[RFC7605] Touch, J., "Recommendations on Using Assigned Transport Port Numbers", BCP 165, RFC 7605, DOI 10.17487/RFC7605, August 2015, <https://www.rfc-editor.org/info/rfc7605>.

[RFC7624] Barnes, R., Schneier, B., Jennings, C., Hardie, T., Trammell, B., Huitema, C., and D. Borkmann, "Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement", RFC 7624, DOI 10.17487/RFC7624, August 2015, <https://www.rfc-editor.org/info/rfc7624>.

[RFC7799] Morton, A., "Active and Passive Metrics and Methods (with Hybrid Types In-Between)", RFC 7799, DOI 10.17487/RFC7799, May 2016, <https://www.rfc-editor.org/info/rfc7799>.

skipping to change at *page 51, line 19* / skipping to change at *page 51, line 19*

-12 Updated following additional feedback from reviewers.

-13 Updated following 2nd WGLC with comments from D.L.Black; T. Herbert; Ekr; and other reviewers.	-13 Updated following 2nd WGLC with comments from D.L.Black; T. Herbert; Ekr; and other reviewers.
-14 Update to resolve feedback to rev -13. This moves the general discussion of adding fields to transport packets to section 6, and discusses with reference to material in RFC8558.	-14 Update to resolve feedback to rev -13. This moves the general discussion of adding fields to transport packets to section 6, and discusses with reference to material in RFC8558.
	-14 Comments from D.L.Black; T. Herbert. Update to add reference to RFC7605.
Authors' Addresses	Authors' Addresses
Godred Fairhurst University of Aberdeen Department of Engineering Fraser Noble Building Aberdeen AB24 3UE Scotland	Godred Fairhurst University of Aberdeen Department of Engineering Fraser Noble Building Aberdeen AB24 3UE Scotland
EMail: gorry@erg.abdn.ac.uk	EMail: gorry@erg.abdn.ac.uk
End of changes. 13 change blocks.	
23 lines changed or deleted	***39 lines changed or added***

This html diff was produced by rfcdiff 1.47. The latest version is available from http://tools.ietf.org/tools/rfcdiff/