Network Working Group
Internet-Draft
Intended status: Informational
Expires: 26 August 2021

J. Arkko
Ericsson

22 February 2021

Considerations on Information Passed between Networks and Applications
draft-arkko-path-signals-information-00

Abstract

Path signals are messages seen by on-path elements examining transport protocols. Current preference for good protocol design indicates desire for constructing explict rather than implicit signals to carry information. For instance, the ability of various middleboxes to read TCP messaging was an implicit signal that lead to difficulties in evolving the TCP protocol without breaking connectivity through some of those middleboxes.

This document discusses the types of information that could be passed in these path signals, and provides some advice on what types of information might be provided in a beneficial manner, and which information might be less likely to be revealed or used by applications or networks.

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 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 26 August 2021.

Copyright Notice

Copyright (c) 2021 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 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.

Table of Contents

1. Introduction

[RFC8558] discusses the topic of path signals: Path signals are messages seen by on-path elements examining transport protocols. There's a difference between implicit and explicit signals. For instance, TCP's well-known messages [RFC0793] are in the clear, and often interpreted in various ways by on-path elements. In contrast, QUIC protects almost all of this information, and hence end-to-end signaling becomes opaque for network elements in between. QUIC does provide some information, but has chosen to make these signals (such as the Spin bit) explicit [I-D.ietf-quic-transport].

Many attempts have been made at network - application collaboration using path signals. Section 2 discusses some of the experiences and guidelines determine from those attempts. This draft then focuses on the specific question of what kind of data can be passed.

2. Past Experiences and Guidance

Incentives are a well understood problem in general but perhaps not fully internalised for various collaborative like designs. The principle is that both receiver and sender of information must acquire tangible and immediate benefits from the communication, such as improved performance,

A related issue is understanding whether there is or is not a business model or ecosystem change. Some designs may work well without any monetary or payment or cross-administrative domains

agreements. For instance, I could ask my packets to be prioritised relative to each other and that shouldn't affect anything else. Some other designs may require a matching business ecosystem change to support what is being proposed, and may be much harder to achieve. For instance, requesting prioritisation over other people's traffic may imply that you have to pay for that which may not be easy even for a single provider let alone across many.

But on to more technical aspects.

The main guidance in [RFC8558] is to be aware that implicit signals will be used whether intended or not. Protocol designers should consider either hiding these signals when the information should not be visible, or using explicit signals when it should be.

[I-D.irtf-panrg-what-not-to-do] discusses many past failure cases, a catalogue of past issues to avoid. It also provides relevant guidelines for new work, from discussion of incentives to more specific observations, such as the need for outperforming end-to-end mechanisms (Section 4.4), considering the need for per-connection state (Section 4.6), and so on.

There are also more general guidance documents, e.g., [RFC5218] discusses protocol successes and failures, and provides general advice on incremental deployability etc. Internet Technology Adoption and Transition (ITAT) workshop report [RFC7305] is also recommended reading on this same general topic. And [RFC6709] discusses protocol extensibility, and provides general advice on the importance of global interoperability and so on.

3. Principles

This section attempts to provide some further guidelines, relating to information that can be passed in path signals. Hopefully, these guidelines can help future designers, explain past issues and recommend useful models to apply.

3.1. Information Specificity

One common problem in finding a workable solution for network - application collaboration is information leakage. All parties are afraid of either their own propietary information or the users' data leaking to others. Oddly enough, no one is usually worried about users' data leaking to themselves, but I digress. :-)

[I-D.per-app-networking-considerations] discusses how applications may be identified through collaboration mechanisms. This can be harmful, as in extreme cases it may lead to undesirable

prioritization decisions or even blocking certain applications. [I-D.per-app-networking-considerations] explains how to reduce the latter problem by categories or requested service rather than specific application identity, such as providing the category "video call service" rather than the name of a particular application performing conference call or video call services. This points to a more general principle of information specificity, providing only the information that is needed for the other party to perform the collaboration task that is desired by this party, and not more. This applies to information sent by an application about itself, information sent about users, or information sent by the network.

An architecture can follow the guideline from RFC 8558 in using explicit signals, but still fail to differentiate properly between information that should be kept private and information that should be shared.

In looking at what information can or cannot easily be passed, we can look at both information from the network to the application, and from the application to the network.

For the application to the network direction, user-identifying information can be problematic for privacy and tracking reasons. Similarly, application identity can be problematic, if it might form the basis for prioritization or discrimination that the that application provider may not wish to happen. It may also have undesirable economic consequences, such as extra charges for the consumer from a priority service where a regular service would have worked.

On the other hand, as noted above, information about general classes of applications may be desirable to be given by application providers, if it enables prioritization that would improve service, e.g., differentiation between interactive and non-interactive services.

For the network to application direction there's less directly sensitive information. Various network conditions, predictive bandwidth and latency capabilities, and so on might be attractive information that applications can use to determine, for instance, optimal strategies for changing codecs.

However, care needs to be take to ensure that neither private information about the individual user (such as user's physical location) is not indirectly exposed through this information. Similarly, this information should not form a mechanism to provide a side-channel into what other users are doing.

3.2. Granularity

In the IAB Covid-19 Network Impacts workshop Jana Iyengar brought up the granularity of operations [I-D.iab-covid19-workshop]. There are many reasons why per-flow designs are problematic: scalability, need to release information about individual user's individual activities, etc. Perhaps designs that work on aggregates would work better.

4. Acknowledgments

The author would like to thank Mirja Kuhlewind, Tommy Pauly, Ted Hardie, David Allan, Brian Trammell, Szilvezter Nadas, Zaheduzzaman Sarker, Joel Halpern, Magnus Westerlund, Jana Iyengar and Balaz Varga for interesting thoughts and proposals in this space.

5. Informative References

[I-D.iab-covid19-workshop]
Arkko, J., Farrell, S., Kuhlewind, M., and C. Perkins, "Report from the IAB COVID-19 Network Impacts Workshop 2020", Internet Draft (Work in Progress), draft-iab-covid19-workshop, IETF , February 2021.

[I-D.ietf-quic-transport]
Iyengar, J. and M. Thomson, "QUIC: A UDP-Based Multiplexed and Secure Transport", Work in Progress, Internet-Draft, draft-ietf-quic-transport-34, 14 January 2021, <https://www.ietf.org/archive/id/draft-ietf-quic-transport-34.txt>.

[I-D.irtf-panrg-what-not-to-do]
Dawkins, S., "Path Aware Networking: Obstacles to Deployment (A Bestiary of Roads Not Taken)", Work in Progress, Internet-Draft, draft-irtf-panrg-what-not-to-do-17, 10 February 2021, <https://www.ietf.org/archive/id/draft-irtf-panrg-what-not-to-do-17.txt>.

[I-D.per-app-networking-considerations]
Colitti, L. and T. Pauly, "Per-Application Networking Considerations", Work in Progress, Internet-Draft, draft-per-app-networking-considerations-00, 15 November 2020, <https://www.ietf.org/archive/id/draft-per-app-networking-considerations-00.txt>.

[RFC0793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981, <https://www.rfc-editor.org/info/rfc793>.

[RFC5218] Thaler, D. and B. Aboba, "What Makes for a Successful Protocol?", RFC 5218, DOI 10.17487/RFC5218, July 2008, <https://www.rfc-editor.org/info/rfc5218>.

[RFC6709] Carpenter, B., Aboba, B., Ed., and S. Cheshire, "Design Considerations for Protocol Extensions", RFC 6709, DOI 10.17487/RFC6709, September 2012, <https://www.rfc-editor.org/info/rfc6709>.

[RFC7305] Lear, E., Ed., "Report from the IAB Workshop on Internet Technology Adoption and Transition (ITAT)", RFC 7305, DOI 10.17487/RFC7305, July 2014, <https://www.rfc-editor.org/info/rfc7305>.

[RFC8558] Hardie, T., Ed., "Transport Protocol Path Signals", RFC 8558, DOI 10.17487/RFC8558, April 2019, <https://www.rfc-editor.org/info/rfc8558>.

Author's Address

Jari Arkko
Ericsson

Email: jari.arkko@ericsson.com