Performance Monitoring in Encrypted Networks: PDMv2

Nalini Elkins: Inside Products, Inc., Mike Ackermann: Blue Cross Blue Shield of Michigan, Mohit P. Tahiliani: NITK Surathkal, Dhruv Dhody: Huawei, India, Prof. Tommaso Pecorella: Università di Firenze, Italy

Abstract

Our proposal is to provide performance information in a uniform way for connections using protocols which encrypt the application payload, such as TLS, without the need to decrypt the payload. This preserves the privacy of the payload. PDMv2 also provides performance information for connections which encrypt the Transport Layer header, such as QUIC, again while preserving the privacy of the payload as well as Transport Header.

Performance Monitoring Tools and Measurement

Measurement and diagnostic tools for performance monitoring differ. Performance monitoring techniques include passive in-line measurement, passive off-line or out-of-band measurement, active monitoring and hybrid (integrates passive and active monitoring).

In discussing performance monitoring, one must also distinguish various measurement types.

- End-to-end user response time
- Server time (CPU time, etc)
- Network time
- Network segment time
- RoundTripTime (TCP, et al)
- TLS handshake time
- Timing measurements for various portions of the protocol (ex. DNS response / request)

IPv6 Performance and Performance and Diagnostic Metrics (PDM)

RFC8250: IPv6 Performance and Diagnostic Metrics (PDM) Destination Option (https://www.rfc-editor.org/rfc/rfc8250.html) proposes a hybrid performance monitoring technique.

"Section 1.2 Rationale for Defined Solution

The current IPv6 specification does not provide timing, nor does it provide a similar field in the IPv6 main header or in any extension header. The IPv6 PDM destination option provides such fields.

Advantages include:

1. Real measure of actual transactions.
2. Ability to span organizational boundaries with consistent instrumentation.
3. No time synchronization needed between session partners.
4. Ability to handle all transport protocols (TCP, UDP, the Stream Control Transmission Protocol (SCTP), etc.) in a uniform way.

PDM provides the ability to determine quickly if the (latency) problem is in the network or in the server (application). That is, it is a fast way to do triage." You may wish to refer to Appendix A of RFC8250 to see why latency and delay calculations are important.

Hybrid Monitoring Models and PDMv2

PDMv2 is a hybrid performance monitoring technique.

PDMv2 provides:

- Round trip delay
- Server delay

Network delay may be deduced or calculated from a combination of round trip and server delay.

Round-trip delay is the delay for packet transfer from a source host to a destination host and then back to the source host. This measurement has been defined, and its advantages and disadvantages are discussed in "A Round-trip Delay Metric for IPPM" [RFC2681]. You may wish to see RFC8250 for a further discussion of server delay as well as scaling.

PDMv2 allows you to do a quick triage to see whether the problem is in the network or the server. For many network operators, this quick triage then allows the right set of technicians to be dispatched. For a further discussion of the importance of triage, please refer to RFC8250.

PDMv2 Measurement Fields

Each packet with PDMv2 contains information about the sender, receiver, delta times and packet sequence numbers. Additionally, PDMv2 contains fields needed for encryption of the PDM header itself. HPKE is used as the methodology.

PDM and PDMv2: Security and Privacy

PDM preserves the privacy of the payload and Transport Header. However, PDM data can be inspected and modified by an on-path adversary. Inspection cannot be detected and can lead to timing attacks, or to the disclosure of vulnerabilities in the infrastructure (e.g., that a server is vulnerable to denial-of-service attacks). Modification also cannot be detected. Modification of PDM data can trigger management actions that can consume resources. E.g., a client (falsely) detecting a bad performance from a server might be forced to switch to a different one, or the server infrastructure to deploy more resources than needed.

PDMv2 preserves the privacy and integrity of PDM by allowing the encryption of the data carried in the extension header. PDMv2 (draft-elkins-ippm-encrypted-pdmv2-02) has been adopted by the IPPM WG.

Performance Information in the Transport Layer

The transport layer headers carry information that can help in monitoring the performance of the network (measuring RoundTripTime) and capabilities of the endpoints (whether multipath support is enabled). Options in TCP header are predominantly used for these purposes. PDM provides the ability to preserve the privacy of this information and determine whether the performance limitations are due to the network constraints or the capabilities of the endpoints.

Encrypted Transport Layer Protocols

QUIC (RFC 9000) is an example of a protocol which encrypts the Transport Layer Header. QUIC is an end-to-end transport protocol implemented as an overlay on a UDP datagram flow. QUIC combines TCP's stream integrity and flow control with encryption from TLS, adds better control over multi-stream handling and works well with NAT.

The initial QUIC handshake combines the typical three-way handshake that you get with TCP/TLS1.3 handshake which provides authentication of the endpoints as well as negotiation of cryptographic parameters. Thus, the connection is always authenticated and encrypted. This has the added benefit of making the initial connection establishment faster. This encryption is performed on the UDP payload, so once the TLS handshake is complete very little of the subsequent QUIC packet exchange is in the clear. Further, by encrypting the additional connection metadata, any abuse by middle-boxes is also prevented.

One of most innovative direction that QUIC takes is to make the fundamental change of placing application layer in charge of transport with security-by-default. What this means to us is that the Transport Layer is encrypted. This poses challenges for network management and diagnostics. PDMv2 attempts to restore performance monitoring for connections using the QUIC protocol. This is only one example of how PDMv2 can work with encrypted protocols.

References

[RFC2681] Almes, G., Kalidindi, S., and Zekauskas, M., "A Round-trip Delay Metric for IPPM", RFC 2681, DOI 10.17487/RFC2681, September 1999, <https://www.rfc-editor.org/info/rfc2681>.

[RFC8250] Elkins, N., Ackermann, M., and Hamilton, R., "IPv6 Performance and Diagnostic Metrics (PDM) Destination Option", RFC 8250, September 2017, <https://www.rfc-editor.org/rfc/rfc8250.html>.

[RFC9000] Ayengar, J., Thomson, M., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, May 2021, <https://datatracker.ietf.org/doc/html/rfc9000>.

[PDMv2] Elkins, N., et al, "IPv6 Performance and Diagnostic Metrics Version 2 (PDMv2) Destination Option",draft-ietf-ippm-encrypted-pdmv2-01, June 2022, <https://datatracker.ietf.org/doc/draft-ietf-ippm-encrypted-pdmv2>.