Problem Statement 02

Secure Network Performance Measurement with Encrypted PDMv2

Reference Documents: draft-ietf-ippm-encrypted-pdmv2-10
Working Group: IPPM

Background

The draft titled *"IPv6 Performance and Diagnostic Metrics Version 2 (PDMv2) Destination Option"* introduces an enhanced performance and diagnostic metric scheme that builds upon RFC 8250. Unlike the original, which embeds timing and sequence data in plaintext—potentially exposing systems to traffic analysis or timing attacks—**Encrypted PDMv2** incorporates a **lightweight handshake (registration)** and **encryption** to protect sensitive measurement metadata. It also introduces **additional performance metrics** for richer diagnostics.

Challenge

Participants are tasked with designing and implementing a **prototype system** that demonstrates a secure, encrypted performance measurement mechanism inspired by Encrypted PDMv2. The goals should revolve around creating a lightweight protocol enabling encrypted diagnostic metadata exchange over IPv6, supporting endpoint registration, and protected measurement.

Possible Focus Areas:

1. **Registration / Handshake Mechanism**
    - Implement a simplified registration flow where a "writer" (sender) and a "reader" (receiver) exchange keys or credentials to establish an encrypted measurement session.
    - Explore appropriate key exchange mechanisms (e.g., HPKE, TLS), being mindful of the draft's identified security details and open questions.
2. **Secure Metadata Exchange**
    - Define and encrypt performance metadata (e.g., sequence numbers, send/receive timestamps) similar to PDMv2's structure.
    - Ensure confidentiality and integrity of transmitted diagnostic data.
3. **Protocol Efficiency & Overhead Analysis**
    - Measure the overhead introduced by encryption and handshake (packet size, latency), referencing the draft's note that added metadata is lightweight and should not significantly impact congestion.
    - Provide analysis comparing clear-text vs. encrypted flows.
4. **Visualization & Analysis Interface**
    - Build a tool or dashboard to visualize performance metrics securely collected (e.g., packet timing graphs, loss/latency trends).
    - Highlight differences in measurement fidelity when compared with standard PDM.

5. **Security Evaluation & Trade-offs**

    ○ Discuss potential threats mitigated (e.g., eavesdropping, timing attacks) and remaining vulnerabilities (ease or difficulty in specifying confidentiality guarantees, insecure handshake design).

Deliverables

- **Prototype Implementation** (CLI tool, server-client app, or web interface) featuring:
    - A registration/h andshake mechanism.
Encrypted transfer of PDM-style metadata over IPv6.
- **Sample Data & Scripts** simulating performance sessions, including both plaintext and encrypted modes.
- **Documentation** covering:
    - Protocol design and flow diagrams of registration and encrypted exchange.
Data format and encryption scheme used.
Analysis of performance overhead and security implications.
Limitations, open questions, and potential enhancements.