New Security Features and Second SEC-DIR (Early) Review

“Test Protocol for One-way IP Capacity Measurement”

draft-ietf-ippm-capacity-metric-protocol-04

L. Ciavattone, A. Morton
Implemented in draft-*-protocol-04, (Dec):

The 04 revision of this new measurement protocol resolves the discussion on Security Modes of Operation. The draft:

• retains the two Authentication modes and the Unauthenticated mode
• adds a new mode for protocol-supported encryption of control/status packets
• adds the option for users to measure within the encrypted tunnel of their choice; this provides fully-encrypted operation (including load/test packets).

The protocol and the running code support measurement of:

• Maximum IP-Layer Capacity Parameter and Method of Measurement (UDP-based test)
• Latency with/without Maximum IP-Layer Load, a.k.a. Working Latency or Responsiveness (we have ALWAYS measured RTT and delay variation, now an opportunity for additional metrics...)
• New Rec. G.1051 Application Traffic stream generation and computation of interactivity factor.
• BBF Quality Experience Delivered (QED) Traffic stream generation, with selected computation to follow.
# Key comments and replies for discussion:

> The use of AES-GCM with a long-lived symmetric key (such as one on an RFC 7210 key chain) is not safe. ... (suggests a CBC mode) ...

  We wanted the "authenticated encryption" aspect of GCM, but we can use **AES-CCM** instead.

  The Initialization Vector (IV) will be random and sent in the clear.

  We need to check if padding is needed for any of our PDUs.

  We will specify the IV generation method.

  **Other Specs needed for Interop** will be derived from required inputs to OpenSSL Lib.
Tension between Security and Measurement operation:

Section 5.1.1 doesn’t say the network addresses and headers are included in the digest. It’s generally good practice to include (them)...

Our test scope includes ISP Subscribers, so NAPT transversal is critical and precludes including the addresses.

... a valid message (e.g., Setup Request) can be extracted/placed in a measurement flow that is not intended by the original sender. This is a substitution attack.

All IPPM test protocols are susceptible to the substitution attack no thorough mitigation (+ time in the digest is a partial mitigation).

Packet De-duplication, in DTLS and IPsec:

This is generally seen as a feature for network encryption methods. Measurement systems expect to observe packet duplication...
# Edits and Nits:
We will take care of other requests for clarifications, etc.

- digest coverage (covers most PDU fields, but not IV)
- MBZ definition
- “Support for client-server authentication ....”.
- four Security modes, but encrypted tunnel makes five? - becomes a paragraph
- mismatch
Next Steps

• More SEC AD and/or SEC-DIR interactions
  • to be sure we are still on-track with the choice of AES-CCM mode and our need for Long-lived Keys.

• WG Last Call on next version, mid 2023?

• Plan to share measurements on the ippm-list:
  • Move this and other work toward conclusion

• UDPST next release: 8.0.0; Single Client Tests with:
  • Multiple flows,
  • Multiple Servers,
  • Resilience to Server failure
Protocol: Setup and Test Phases
draft-ietf-ippm-capacity-metric-protocol-03

**Communication to Well-Known Port (REQUIRED AUTH)**

- Client: Add authDigest on Request/Reply

**Communication to Ephemeral Port**

- Setup Exchange
- Test Activation Exchange

**Request PDU**

- Check AUTH
- Allocate Test Socket
- Reply Includes Ephemeral Port
- Server Admission Control: BW check
- ADD authDigest and Processing on Reply
- ADD outgoing packet to open Ephemeral Port on FW
- Affirm or Replace Testing Parameters (Down/Up, duration, etc.)

**Response PDU**

- CONTROL Phase
- DATA Phase
- Feedback at 50ms intervals (def): Measurements (loss, delay, Rcv Rate)
- OR Sending Rate Structure
- ADD authDigest and Processing - OPTIONAL

**Test Stream & Feedback PDUs**

- Not shown:
- Test STOP in Load PDU:
- ADD authDigest & Processing?
- NO – processing issue!

**Load PDUs**

- Time stamps, SeqNums, up to 40 Gbps rates