

A One-way Delay Measurement Protocol

draft-ietf-ippm-owdp

S. Shalunov, B. Teitelbaum, M. Zekauskas

49th IETF, San Diego, December 2000

Goals

- Design a protocol that can be used for collection of one-way statistics defined in RFC 2679 and RFC 2680.
- Protocol usable in a wide range of scenarios: from one-way ping to network monitoring in the style of IPPM Surveyor and RIPE Test Traffic.
- Stealth: hard for ISPs to detect.
- Security: authentication, integrity protection.
- Try to fit into a single ATM cell.

OWDP-Control vs. OWDP-Test

Two related protocols are defined: OWDP-Control and OWDP-Test.

OWDP-Test is the actual test traffic stream. (UDP packets using negotiated port numbers, average rate, and packet size.)

OWDP-Control is used to schedule, start, and stop OWDP-Test sessions and retrieve their results. (TCP connection to a well-known port number.) Commands available in an OWDP-Control session: Request-Session, Start-Sessions, Stop-Sessions, Retrieve-Session. Multiple OWDP-Test sessions can be scheduled using the same OWDP-Control connection.

Logical Roles

Session-Sender the sender of an OWDP-Test session;

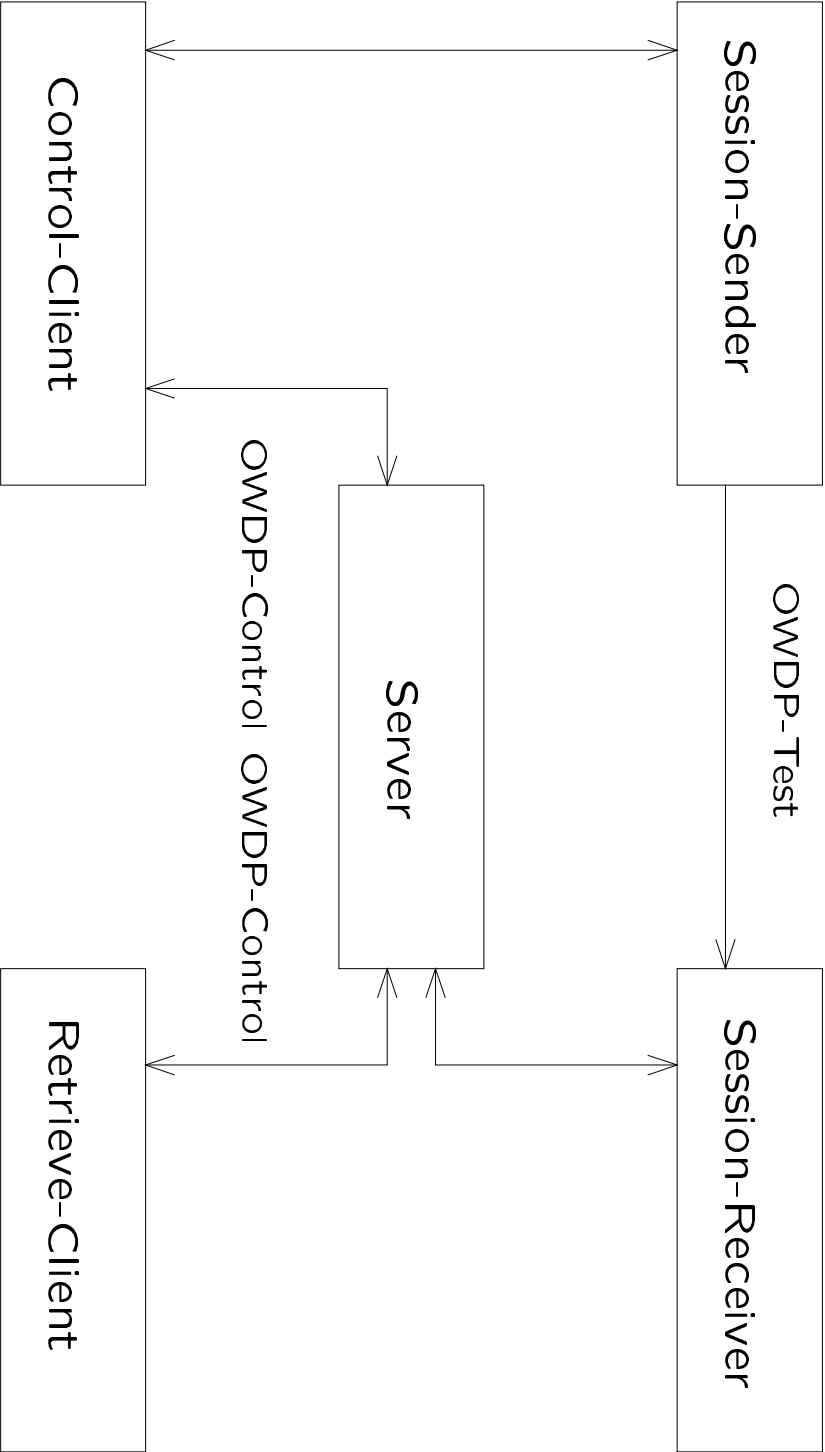
Session-Receiver the receiver of an OWDP-Test session;

Server OWDP-Control server: manages OWDP-Test sessions;

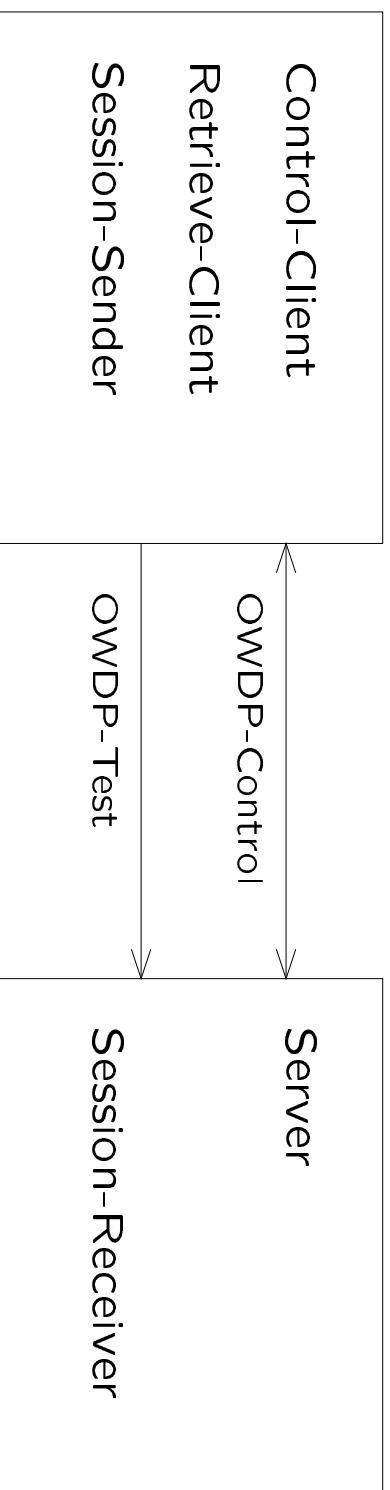
Control-Client OWDP-Control client: ditto;

Retrieve-Client OWDP-Control client: retrieves session results.

One scenario of relationships



Several roles can be played by one host



Here, Server (Session-Receiver) could be an open server and Client (Session-Sender) could be a casual user who wants to check his connectivity to the server.

Unauthenticated, Authenticated, Encrypted

Unauthenticated Open mode, suitable for servers and clients that are complete strangers.

Authenticated Requires shared secret. Provides access control. Allows senders and receivers to screen bogus messages from would-be attackers that cannot observe OWDP-Test traffic. Timestamps themselves (in OWDP-Test) aren't encrypted.

Encrypted Additionally, provides integrity and secrecy against attackers between the client and the server. Differs from authenticated mode only in OWDP-Test.

Both secrecy and integrity are provided by AES block cipher.

OWDPP-Test

A Poisson stream (with negotiated parameter) of UDP packets from negotiated port on Session-Sender to negotiated port on Session-Receiver is sent.

The packet just includes a 4-octet sequence number and an 8-octet timestamp (NTP-style). This allows to fit into one ATM cell (20 octets of UDP packet body) in unauthenticated and encrypted modes and still have some space for authentication.

In encrypted mode, the interesting part is one 16-octet AES block. In authenticated mode, the interesting part is 16 octet block of authentication info plus 8-octet timestamp.

In all modes, fixed amount of padding is appended, filled with arbitrary pseudo-random data (or zeros).

OWDP-Control

An OWDP-Control listens on a well-known TCP port. A client, once connected, negotiates mode and authenticates, if necessary. Further exchanges are encrypted using a session key; encryption is done in such a manner as to allow for integrity checking of each message.

A client then can either set up and ask to conduct OWDP-Test sessions, or retrieve results of old sessions. Sessions are characterized by session IDs (SIDs). SIDs are globally unique in the same way RFC 822 Message-IDs should be.

Comments from IPPM mailing list

- Make padding pseudo-random/arbitrary. *Done.*
- Make it clear that OWDP-Test can be used without OWDP-Control. *Prose changes only?*
- Add options to set DF, TTL, DSCP. *Under discussion.*
- Add options to negotiate periodic and uniformly distributed OWDP-Test streams. *Under discussion.*

New version (-01) has been submitted for publication as an IPPM WG draft and will appear in the ID repository as soon as it is re-opened. *Your opinion on last two bullets?*

For Additional Information...

<http://www.ietf.org/internet-drafts/draft-ietf-ippm-owdp-00.txt>

<http://www.internet2.edu/~shalunov/draft-ietf-ippm-owdp-01.txt>

Stanislav Shalunov <shalunov@internet2.edu>

Benjamin Teitelbaum <ben@advanced.org>

Matthew J. Zekauskas <matt@advanced.org>

Questions?