Network Working Group	A. Morton	
Internet-Draft	AT&T Labs	
Intended status: Standards Track	K. Hedayat	
Expires: April 23, 2009	Brix Networks	
	October 20, 2008	

TOC

More Features for TWAMP
draft-ietf-ippm-more-twamp-00

Status of this Memo

Abstract

The IETF has completed its work on TWAMP - the Two-Way Active Measurement Protocol. This memo describes a simple extension to TWAMP, the option to use different security modes in the TWAMP-Control and TWAMP-Test protocols.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.) [RFC2119].

Table of Contents

1. Introduction

TOC

The IETF has completed its work on the core specification of TWAMP - the Two-Way Active Measurement Protocol [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.). TWAMP is an extension of the One-way Active Measurement Protocol, OWAMP [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)," September 2006.). The TWAMP specification gathered wide review as it approached completion, and the by-products were several recommendations for new features in TWAMP. There are a growing number TWAMP implementations at present, and wide-spread usage is expected. There are even devices that are designed to test implementations for protocol compliance.

This memo describes a simple extension for TWAMP, the option to use different security modes in the TWAMP-Control and TWAMP-Test protocols. The relationship between this memo and TWAMP is intended to be an update to [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.) when published.

2. Purpose and Scope

TOC

The purpose of this memo is to describe and specify an extension for TWAMP [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.). The features and extensions were vetted before adoption in this memo.
The scope of the memo is limited to specifications of the following:

*Extension of the modes of operation through assignment of one new value in the Mode field (see section 3.1 of [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)," September 2006.)), while retaining backward compatibility with TWAMP [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.) implementations. This value adds the OPTIONAL ability to use different security modes in the TWAMP-Control and TWAMP-Test protocols. The motivation for this extension is to permit the low packet rate TWAMP-Control protocol to utilize a stronger mode of integrity protection than that used in the TWAMP-Test protocol.

3. TWAMP Control Extensions

TOC

TWAMP-Control protocol is a derivative of the OWAMP-Control protocol, and coordinates a two-way measurement capability. All TWAMP Control messages are similar in format and follow similar guidelines to those defined in section 3 of [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)," September 2006.) with the exceptions described in TWAMP [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.), and in the following sections.
All OWAMP-Control messages apply to TWAMP-Control, except for the Fetch Session command.

3.1. Extended Connection Setup

TOC

TWAMP connection establishment follows the same procedure defined in section 3.1 of [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A.,

Boote, J., and M. Zekauskas, “A One-way Active Measurement Protocol (OWAMP),” September 2006.). This extended mode assigns one new bit position (and value) to allow the Test protocol security mode to operate in Unauthenticated mode, while the Control protocol operates in Encrypted mode. With this extension, the complete set of TWAMP values are as follows:

Value	Description	Reference/Explanation
0	Reserved	
1	Unauthenticated	RFC4656, Section 3.1
2	Authenticated	RFC4656, Section 3.1
4	Encrypted	RFC4656, Section 3.1
8	Unauth. TEST protocol, Encrypted CONTROL	new bit position (3)

In the original OWAMP Modes field, setting bit positions 0, 1 or 2 indicated the security mode of the Control protocol, and the Test protocol inherited the same mode (see section 4 of [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, “A One-way Active Measurement Protocol (OWAMP),” September 2006.)). In this extension to TWAMP, setting Modes Field bit position 3 SHALL discontinue the inheritance of the security mode in the Test protocol, and each protocol’s mode SHALL be as specified below. When the desired TWAMP Test protocol mode is identical to the Control Session mode, the corresponding Modes Field bit (position 0, 1 or 2) SHALL be set. The table below gives the various combinations of integrity protection that are permissible in TWAMP (with this extension). The Test protocol SHALL use the mode in each column corresponding to the Modes Field bit position.

Protocol	Permissible Mode Combinations (Modes bit set)	
Control	Unauth.(0)	Auth. == Encrypted (1,2,3)
Test	Unauth.(0)	Unauth. (3)
		Auth.(1)
		Encrypted (2)

Note that the TWAMP-Control protocol security measures are identical in the Authenticated and Encrypted Modes. Therefore, only one new bit position (3) is needed to convey the single mixed security mode.
The value of the Modes Field sent by the Server in the Server-Greeting message is the bit-wise OR of the modes (bit positions) that it is willing to support during this session. Thus, the last four bits of the Modes 32-bit Field are used. The first 28 bits MUST be zero. A client

conforming to this extension of [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.) MAY ignore the values in the first 28 bits of the Modes Field, or it MAY support other features that are communicated in these bit positions.
Other ways in which TWAMP extends OWAMP are described in [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.).

---

4. Extended TWAMP Test

TOC

The TWAMP test protocol is similar to the OWAMP [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)," September 2006.) test protocol with the exception that the Session-Reflector transmits test packets to the Session-Sender in response to each test packet it receives. TWAMP [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.) defines two different test packet formats, one for packets transmitted by the Session-Sender and one for packets transmitted by the Session-Reflector. As with OWAMP-Test protocol there are three security modes: unauthenticated, authenticated, and encrypted. This TWAMP extension makes it possible to use TWAMP-Test Unauthenticated mode regardless of the mode used in the TWAMP-Control protocol.

4.1. Sender Behavior

TOC

This section describes REQUIRED extensions to the behavior of the TWAMP Sender.

4.1.1. Packet Timings

TOC

The Send Schedule is not utilized in TWAMP, and there are no extensions defined in this memo.

TOC

4.1.2. Packet Format and Content

The Session Sender packet format and content MUST follow the same procedure and guidelines as defined in section 4.1.2 of [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)," September 2006.) and section 4.1.2 of [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.), with the following exceptions:

*the Send Schedule is not used, and

*the Sessions-Sender MUST support the mixed security mode (Unauthenticated TEST, Encrypted CONTROL,value 8, bit position 3) defined in section 3.1 of this memo.

4.2. Reflector Behavior

TOC

The TWAMP Reflector is REQUIRED to follow the procedures and guidelines in section 4.2 of [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.), with the following extensions:

*the Sessions-Reflector MUST support the mixed security mode (Unauthenticated TEST, Encrypted CONTROL,value 8, bit position 3) defined in section 3.1 of this memo.

---

5. Security Considerations

TOC

The extended mixed-mode of operation permits stronger security/ integrity protection on the TWAMP-Control protocol while simultaneously emphasizing accuracy or efficiency on the TWAMP-Test protocol, thus making it possible to increase overall security when compared to the previous options.
The security considerations that apply to any active measurement of live networks are relevant here as well. See [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)," September 2006.) and [RFC5357] (Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)," October 2008.).

---

6. IANA Considerations

TOC

This memo adds three security mode combinations to the OWAMP-Control specification[RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, “A One-way Active Measurement Protocol (OWAMP),” September 2006.), and describes behavior when the new modes are used. This memo requests creation an IANA registry for the TWAMP Mode field. This field is a recognized extension mechanism for TWAMP.

6.1. Registry Specification

TOC

IANA is requested to create a TWAMP-Modes registry. TWAMP-Modes are specified in TWAMP Server Greeting messages and Set-up Response messages consistent with section 3.1 of [RFC4656] (Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, “A One-way Active Measurement Protocol (OWAMP),” September 2006.), and extended by this memo. Modes are indicated by setting bits in the 32-bit Modes Field. Thus, this registry can contain a total of 32 possible bit positions and corresponding values.

6.2. Registry Management

TOC

Because the TWAMP-Modes registry can contain only thirty-two values, and because TWAMP is an IETF protocol, this registry must be updated only by "IETF Consensus" as specified in [RFC2434] (Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” October 1998.)(an RFC documenting registry use that is approved by the IESG). For the Modes registry, we expect that new features will be assigned using monotonically increasing bit positions and in the range [0-31] and the corresponding values, unless there is a good reason to do otherwise.

6.3. Experimental Numbers

TOC

No experimental values are currently assigned for the Modes Registry.

TOC

6.4. Initial Registry Contents

TWAMP Modes Registry

Value	Description	Semantics Definition
0	Reserved	
1	Unauthenticated	RFC4656, Section 3.1
2	Authenticated	RFC4656, Section 3.1
4	Encrypted	RFC4656, Section 3.1
8	Unauth. TEST protocol, Encrypted CONTROL	this document, Section 3.1

7. Acknowledgements

TOC

The authors would like to thank Len Ciavattone for helpful review and comments.

8. References

TOC

8.1. Normative References

TOC

[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC2434]	Narten, T. and H. Alvestrand, “Guidelines for Writing an IANA Considerations Section in RFCs,” BCP 26, RFC 2434, October 1998 (TXT, HTML, XML).
[RFC4656]	Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, “A One-way Active Measurement Protocol (OWAMP),” RFC 4656, September 2006 (TXT).
[RFC5357]	Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, “A Two-Way Active Measurement Protocol (TWAMP),” RFC 5357, October 2008 (TXT).

8.2. Informative References

TOC

[x]	“.”

Authors' Addresses

TOC

	Al Morton
	AT&T Labs
	200 Laurel Avenue South
	Middletown,, NJ 07748
	USA
Phone:	+1 732 420 1571
Fax:	+1 732 368 1192
Email:	acmorton@att.com
URI:	http://home.comcast.net/~acmacm/
	Kaynam Hedayat
	Brix Networks
	285 Mill Road
	Chelmsford, MA 01824
	USA
Phone:	+1
Fax:	+1
Email:	khedayat@brixnet.com
URI:	http://www.brixnet.com/

Full Copyright Statement

TOC

Intellectual Property

pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.