Network Working Group
Request for Comments: 5618
Updates: 5357
Category: Standards Track

A. Morton
AT&T Labs
K. Hedayat
EXFO

August 2009

Mixed Security Mode for the Two-Way Active Measurement Protocol (TWAMP)

Abstract

This memo describes a simple extension to TWAMP (the Two-Way Active Measurement Protocol). The extension adds the option to use different security modes in the TWAMP-Control and TWAMP-Test protocols simultaneously. The memo also describes a new IANA registry for additional features, called the TWAMP Modes registry.

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Table of Contents

1. Introduction

The Two-Way Active Measurement Protocol (TWAMP) [RFC5357] is an extension of the One-Way Active Measurement Protocol (OWAMP) [RFC4656]. The TWAMP specification gathered wide review as it approached completion, and the by-products were several recommendations for new features in TWAMP. There is a growing number of TWAMP implementations at present, and widespread 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 (mixed security mode). It also describes a new IANA registry for additional features, called the TWAMP Modes registry.

When the Server and Control-Client have agreed to use the mixed security mode during control connection setup, then the Control-Client, the Server, the Session-Sender, and the Session-Reflector MUST all conform to the requirements of this mode as described in Sections 3, 4, and 5.

This memo updates [RFC5357].

1.1. 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 [RFC2119].

2. Purpose and Scope

The purpose of this memo is to describe and specify an extension for TWAMP [RFC5357], and to request the establishment of a registry for future TWAMP extensions.

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 Modes field (see Section 3.1 of [RFC4656]), while retaining backward compatibility with TWAMP [RFC5357] 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

The 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], with the exceptions described in TWAMP [RFC5357] and in the following sections.

All OWAMP-Control messages apply to TWAMP-Control, except for the Fetch-Session command.

3.1. Extended Control Connection Setup

TWAMP-Control connection establishment follows the same procedure defined in Section 3.1 of [RFC4656]. 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 Mode values are as follows:

Value	Description	Reference/Explanation
0	Reserved	
1	Unauthenticated	RFC 4656, Section 3.1
2	Authenticated	RFC 4656, Section 3.1
4	Encrypted	RFC 4656, Section 3.1
8	Unauth. TEST protocol, Encrypted CONTROL	new bit position (3)

In the original OWAMP and TWAMP Modes field, setting bit position 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]).

In this extension to TWAMP, when the Control-Client sets Modes Field bit position 3, it 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 by the Control-Client. The table below gives the various combinations of integrity protection that are permissible in TWAMP (with this extension). The TWAMP-Control and TWAMP-Test protocols SHALL use the mode in each column corresponding to the bit position set in the Modes Field.

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 32-bit Modes Field are used. When no other features are activated, the first 28 bits MUST be zero. A client conforming to this extension of [RFC5357] 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].

4. Extended TWAMP Test

The TWAMP-Test protocol is similar to the OWAMP-Test protocol [RFC4656] with the exception that the Session-Reflector transmits test packets to the Session-Sender in response to each test packet it receives. TWAMP [RFC5357] 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 the OWAMP-Test protocol, there are three security modes that also determine the test packet format: 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.

When the Server has identified the ability to support the mixed security mode, the Control-Client has selected the mixed security mode in its Set-Up-Response, and the Server has responded with a zero Accept field in the Server-Start message, these extensions are REQUIRED.

4.1. Sender Behavior

This section describes extensions to the behavior of the TWAMP Session-Sender.

4.1.1. Packet Timings

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

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] and Section 4.1.2 of [RFC5357], with the following exceptions:

- the send schedule is not used, and
- the Session-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

The TWAMP Session-Reflector is REQUIRED to follow the procedures and guidelines in Section 4.2 of [RFC5357], with the following extensions:

- the Session-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

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 (when resource constraints would have forced less security for TWAMP-Control and conditions are such that use of unauthenticated TWAMP-Test is not a significant concern).

The security considerations that apply to any active measurement of live networks are relevant here as well. See [RFC4656] and [RFC5357].

6. IANA Considerations

This memo adds one security mode bit position/value beyond those in the OWAMP-Control specification [RFC4656], and describes behavior when the new mode is used. According to this document, IANA created a registry for the TWAMP Modes field. This field is a recognized extension mechanism for TWAMP.

6.1. Registry Specification

IANA created 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] and Section 3.1 of [RFC5357], and extended by this memo. Modes are currently indicated by setting single bits in the 32-bit Modes Field. However, more complex encoding may be used in the future. Thus, this registry can contain a total of 2^32 possible assignments.

6.2. Registry Management

Because the TWAMP Modes registry can contain a maximum of 2^32 values, and because TWAMP is an IETF protocol, this registry must be updated only by "IETF Review" as specified in [RFC5226] (an RFC documenting registry use that is approved by the IESG). For the

TWAMP Modes registry, we expect that new features will be assigned using monotonically increasing single bit positions and in the range [0-31], unless there is a good reason to do otherwise (more complex encoding than single bit positions may be used in the future, to access the 2^32 value space).

6.3. Experimental Numbers

No experimental values are currently assigned for the Modes Registry.

6.4. Initial Registry Contents

TWAMP Modes Registry

Value	Description	Semantics Definition
0	Reserved	RFC 5618
1	Unauthenticated	RFC 4656, Section 3.1
2	Authenticated	RFC 4656, Section 3.1
4	Encrypted	RFC 4656, Section 3.1
8	Unauth. TEST protocol, Encrypted CONTROL	RFC 5618, Section 3.1

7. Acknowledgements

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

8. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4656] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)", RFC 4656, September 2006.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5357] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)", RFC 5357, October 2008.

Authors' Addresses

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
EXFO
285 Mill Road
Chelmsford, MA 01824
USA

Phone: +1 978 367 5611
Fax: +1 978 367 5700
EMail: kaynam.hedayat@exfo.com
URI: http://www.exfo.com/