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)

Смешанный режим защиты для протокола TWAMP

Аннотация

Этот документ описывает простое расширение протокола двухстороннего активного измерения (Two-Way Active Measurement Protocol или TWAMP), добавляющее опция использования различных механизмов защиты в протоколах TWAMP-Control и TWAMP-Test одновременно. Документ также описывает новый рреестр IANA для дополнительных функций (TWAMP Modes).

Статус документа

Это документ содержит проект стандарта протокола Internet для сообщества Internet и служит приглашением к дискуссии в целях развития и совершенствования протокола. Текущее состояние стандартизации и статус протокола можно узнать из текущей версии документа Internet Official Protocol Standards (STD 1). Допускается свободное распространение документа.

Оглавление

1. Введение

Протокол TWAMP [RFC5357] является расширением протокола односторонних активных измерений (One-Way Active Measurement Protocol или OWAMP) [RFC4656]. Спецификация TWAMP прошла широкое обсуждение, в процессе которого были предложены несколько рекомендаций по новым функциям TWAMP. В настоящее время число реализаций TWAMP растет и ожидается их широкое использование. Разработаны даже устройства, предназначенные для проверки соответствия реализаций протоколу.

В этом документе описано простое расширение TWAMP - опция для использования разных режимов защиты в протоколах TWAMP-Control и TWAMP-Test (смешанная защита). Документ также описывает новый реестр IANA для дополнительных функций, названный TWAMP Modes.

Когда Server и Control-Client согласовали использование смешанного режима защиты в процессе организации соединения, Control-Client, Server, Session-Sender и Session-Reflector **должны** соответствовать требованиям к этому режиму, указанным в разделах 3 - 5.

Этот документ обновляет [RFC5357].

1.1. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с RFC 2119 [RFC2119].

2. Назначение и область действия

Назначение этого документа состоит в описании и спецификации расширения для протокола TWAMP [RFC5357] и запросе на создание реестра для будущих расширений TWAMP.

Область действия документа ограничена спецификацией указанного ниже расширения.

- Расширение режимов работы путем выделения нового значения поля Modes (параграф 3.1 в [RFC4656]) при сохранении совместимости с имеющимися реализациями TWAMP [RFC5357]. Это значение добавляет **необязательную** возможность применять разные режимы защиты для протоколов TWAMP-Control и TWAMP-Test. Расширение предназначено для обеспечения протоколу TWAMP-Control, имеющему низкую скорость передачи пакетов, возможности применять более строгую защиту по сравнению с используемой TWAMP-Test.

3. Расширения TWAMP-Control

Протокол TWAMP-Control основан на OWAMP-Control и координирует двухсторонние измерения. Все сообщения TWAMP-Control, за исключением отмеченных в TWAMP [RFC5357] и последующих параграфах, похожи по формату на сообщения, определенные в разделе 3 [RFC4656], и следуют рекомендациям указанного документа.

Все сообщения OWAMP-Control, за исключением команды Fetch-Session, применимы к протоколу TWAMP-Control.

3.1. Организация расширенного управляющего соединения

При организации управляющих соединений TWAMP-Control используется процедура, описанная в параграфе 3.1 [RFC4656]. Это расширенный режим использует дополнительный бит, позволяющий разрешить протоколу TWAMP-Test работать в режме без аутентификации (Unauthenticated), тогда как протокол TWAMP-Control работает в режиме с шифрованием (Encrypted). Полный набор значений TWAMP Mode с учетом этого расширения показан в таблице.

Значение	***Описание***	***Определение семантики***
0	Резерв	
1	Unauthenticated	RFC 4656, параграф 3.1
2	Authenticated	RFC 4656, параграф 3.1
4	Encrypted	RFC 4656, параграф 3.1
8	Unauthenticated для протокола Test, Encrypted для Control	Новая битовая позиция (3)

В исходном поле Modes протоколов OWAMP и TWAMP установка бита 0, 1 или 2 задает режим защиты для протокола управления (Control), а протокол тестирования (Test) наследует этот режим (раздел 4 в [RFC4656]).

В этом расширении TWAMP при установке клиентом (Control-Client) в поле Modes битп 3, клиенту **нужно** предотвратить наследование режима защиты протоколом Test, при этом для каждого из протоколов **нужно** устанавливать режим в соответствии с приведенным ниже описанием. Если для протокола TWAMP-Test нужен такой же режим защиты как для сеанса управления, клиенту **нужно** устанавливать соответствующий режим (биты 0 - 2) в поле Modes. Приведенная ниже таблица показывает различные комбинации режимов защиты целостности, доступные в TWAMP с этим расширением. Протоколам TWAMP-Control и TWAMP-Test **нужно** применять режим, указанный в столбце, соответствующем битам поля Modes.

Протокол	***Возможные комбинации режимов (биты Modes)***	
Control	Unauthenticated (0)	Authenticated == Encrypted (1,2,3)
Test	Unauthenticated (0)	Unauthenticated (3) Authenticated (1) Encrypted (2)

Отметим, что меры защиты протокола TWAMP-Control идентичны в режимах Authenticated и Encrypted, поэтому для смешанного режима достаточно одной битовой позиции (3).

Значение поля Modes передаются сервером в сообщении Server-Greeting как результат объединения (OR) битов для режимов, которые будут поддерживаться в этой сессии. В результате используются 4 последних бита 32-битового поля Modes. Когде ни используется никаких иных функций, первые 28 битов **должны** быть сброшены (0). Клиент, соответствующий данному расширению [RFC5357], **может** игнорировать первые 28 битов поля Modes или **может** поддерживать другие функции, указываемые этими битами.

Другие способы расширения в TWAMP протокола OWAMP описаны в [RFC5357].

4. Расширенный протокол TWAMP-Test

Протокол TWAMP-Test подобен OWAMP-Test [RFC4656] за исключением того, что Session-Reflector передает пакеты отправителю (Session-Sender) в ответ на каждый принятый пакет. TWAMP [RFC5357] определяет два формата тестовых пакетов, один из которых использует при передаче Session-Sender, другой - Session-Reflector. Как и в протоколе OWAMP-Test, здесь поддерживается 3 режима защиты, которые влияют на формат пакетов, - без аутентификации, с аутентификацией и с шифрованием. Данное расширение TWAMP делает возможным использование режима TWAMP-Test Unauthenticated независимо от режима протокола TWAMP-Control.

Это расширение **требуется**, когда Server указал возможность поддержки смешанного режима защиты, Control-Client выбрал этот режим в своем сообщении Set-Up-Response и сервер ответил сообщением Server-Start с Accept = 0.

4.1. Поведение отправителя

В этом параграфе описаны расширения в поведении TWAMP Session-Sender.

4.1.1. Тактирование пакетов

Планирование передачи не применяется в TWAMP и этот документ не задает расширений.

4.1.2. Формат и содержимое пакетов

Формат и содержимое пакетов Session-Sender **должны** следовать процедуре и рекомендациям параграфов 4.1.2 в [RFC4656] и 4.1.2 в [RFC5357] с учетом отмеченных ниже исключений:

- планирование передачи не применяется;
- Session-Sender **должен** поддерживать смешанный режим (Unauthenticated TEST, Encrypted CONTROL, значение 8, бит 3), определенный в параграфе 3.1 этого документа.

4.2. Поведение рефлектора

От TWAMP Session-Reflector **требуется** следовать процедуре и рекомендациям параграфа 4.2 в [RFC5357] с одним исключением:

- Session-Reflector **должен** поддерживать смешанный режим (Unauthenticated TEST, Encrypted CONTROL, значение 8, бит 3), определенный в параграфе 3.1 этого документа.

5. Вопросы безопасности

Смешанный режим защиты обеспечивает строгую защиту целостности для протокола TWAMP-Control, одновременно повышая точность и эффективность протокола TWAMP-Test, позволяя повысить общий уровень безопасности по сравнению с прежними вариантами (когда ограничение ресурсов приводили к снижению уровня защиты TWAMP-Control в условиях, когда использование TWAMP-Test без аутентификации не вызывало проблем).

К этому документу применимы вопросы безопасности, связанные с активными измерениями в работающих сетях (см. [RFC4656] и [RFC5357]).

6. Взаимодействие с IANA

Этот документ добавляет бит (и значение) выбора режима защиты в дополнение к указанным в спецификации OWAMP-Control [RFC4656] и определяет поведение при использовании этого режима. В соответствии с этим документом создан реестр IANA для поля TWAMP Modes, признанного механизмом расширения для протокола TWAMP.

6.1. Спецификация реестра

Агентство IANA создало реестр TWAMP Modes. Значение TWAMP Modes указывается в сообщениях TWAMP Server Greeting и Set-up Response, соответствующих параграфам 3.1 в [RFC4656] и 3.1 в [RFC5357] и расширенных этим документом. Режимы в настоящее время устанавливаются отдельными битами 32-битового поля Modes. Однако в будущем кодирование может быть усложнено. Таким образом, реестр может включать до 2^{32} разных значений.

6.2. Управление реестром

Поскольку реестр TWAMP Modes может включать до 2^{32} значений, а TWAMP является протоколом IETF, обновление реестра выполняется по процедуре IETF Review, описанной в [RFC5226] (RFC с документированием использования реестра, одобренный IESG). Для реестра TWAMP Modes предполагается выделение значений с ростом битовой позиции (0-31), если не будет веской причины использовать другой подход (более сложное кодирование, которое может быть выбрано в будущем для доступа ко всему пространству из 2^{32} значений).

6.3. Экспериментальные значения

В настоящее время реестр Modes не включает экспериментальных значений.

6.4. Начальное содержимое реестра

Реестр TWAMP Modes показан в таблице.

Значение	*Описание*	*Определение семантики*
0	Резерв	RFC 5618
1	Unauthenticated	RFC 4656, параграф 3.1
2	Authenticated	RFC 4656, параграф 3.1
4	Encrypted	RFC 4656, параграф 3.1
8	Unauthenticated TEST, Encrypted CONTROL	RFC 5618, параграф 3.1

7. Благодарности

Авторы благодарят Len Ciavattone и Joel Jaeggli за полезные комментарии и рецензии.

8. Нормативные документы

[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.

Адреса авторов

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/

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru