Network Working Group
Request for Comments: 5425
Category: Standards Track

F. Miao, Ed.
Y. Ma, Ed.
Huawei Technologies
J. Salowey, Ed.
Cisco Systems, Inc.

March 2009

Транспортное отображение TLS для Syslog

Transport Layer Security (TLS) Transport Mapping for Syslog

Статус документа

Этот документ является проектом стандарта Internet (Internet Standards Track) и служит приглашением к дискуссии и внесению предложений с целью совершенствования протокола. Информацию о состоянии стандартизации и статусе протокола можно найти в текущей редакции документа «Internet Official Protocol Standards» (STD 1). Документ может распространяться свободно.

Авторские права

Аннотация

В этом документе описано использование защиты транспортного уровня (TLS[3]) для обеспечения защиты соединений, служащих для транспортировки сообщений syslog. Описаны угрозы безопасности syslog и способы использования TLS для преодоления таких угроз.

Оглавление

[1] В оригинале - IETF Contributions. *Прим. перев.*
[2] В оригинале - IETF Standards Process. *Прим. перев.*
[3] Transport Layer Security

1. Введение

В этом документе описано использование защиты транспортного уровня (TLS [RFC5246]) для обеспечения защиты соединений, служащих для транспортировки сообщений syslog. Описаны угрозы безопасности syslog и способы использования TLS для преодоления таких угроз.

1.1. Терминология

Ниже приведены определения используемых в документе терминов.

- «инициатор» (originator) генерирует содержимое для передачи в сообщениях syslog;
- «коллектор» (collector) собирает содержимое сообщений syslog для дальнейшего анализа;
- «транслятор» (relay) пересылает сообщения, воспринимает сообщения от инициатора или других трансляторов и передаёт их коллекторам или другим трансляторам;
- «транспортный отправитель» (transport sender) передаёт сообщения syslog заданному транспортному протоколу;
- «транспортный получатель» (transport receiver) принимает сообщения syslog от заданного транспортного протокола;
- клиент TLS - приложение, которое может инициировать соединение TLS, передавая серверу Client Hello;
- сервер TLS - приложение, которое может принимать сообщения Client Hello от клиентов и отвечать на низ сообщениями Server Hello.

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. Требования безопасности для Syslog

Сообщения Syslog на пути к коллектору могут проходить через несколько интервалов пересылки (hop). Некоторые из промежуточных сетей могут не быть доверенными для инициатора, транслятора или коллектора по причине того, что эти сети относятся к другим доменам безопасности или имеют уровень защиты, отличающийся от уровня для инициатора, транслятора или коллектора. Другим вопросом безопасности является размещение самого инициатора, транслятора или коллектора в незащищённой сети.

Имеется несколько угроз, которые требуется учитывать в плане безопасности syslog. Основные из них указаны ниже.

- Маскировка. Неуполномоченный транспортный отправитель может передавать сообщения легитимному транспортному получателю или неуполномоченный транспортный получатель может попытаться обмануть легитимного транспортного отправителя с целью получения от того сообщений syslog.
- Изменение. Атакующий, расположенный между транспортными отправителем и получателем, может изменять передаваемые сообщения syslog и после этого пересылать их транспортному получателю. Такие изменения могут сделать сообщения непонятными транспортному получателю или изменить его поведение нежелательным образом.
- Раскрытие. Неуполномоченный элемент может просматривать содержимое сообщений syslog, получая несанкционированный доступ к информации. Некоторые данные в сообщениях syslog являются «деликатными» и могут помочь атакующему в его деятельности (например, пароли администраторов или уполномоченных пользователей).

Другая угроза описана ниже.

- Изменение потока сообщений. Атакующий может удалить одно или несколько сообщений syslog из последовательности, повторно использовать сообщения или поменять порядок их доставки. Сам протокол syslog не поддерживает порядка сообщений. Однако события, указанные в сообщениях syslog, могут быть семантически связанными с событиями из других сообщений и порядок доставки может быть важен для понимания порядка событий.

Ниже перечислены угрозы, которые считаются менее важными для syslog и не рассматриваются в этом документе.

- Отказ в обслуживании;
- анализ трафика.

3. Применение TLS для защиты Syslog

TLS можно использовать в качестве защищённого транспорта с учётом всех перечисленных выше основных угроз:

- защита конфиденциальности для предотвращения раскрытия содержимого сообщений;
- контроль целостности для предотвращения изменения сообщений в процесс пересылки;
- аутентификация сервера или взаимная аутентификация для предотвращения маскировки.

Примечание. Этот транспорт (т. е., TLS) защищает syslog поэтапно (hop-by-hop) и не связан с содержимым сообщений syslog. В частности, подтверждённая идентификация транспортного отправителя (например, имя субъекта в сертификате) не обязательно относится к полю HOSTNAME в сообщении syslog. Если нужна проверка подлинности источника сообщений syslog, можно использовать [SYS-SIGN].

4. Элементы протокола

4.1. Выделение портов

Транспортный отправитель syslog всегда является клиентом TLS, а транспортный получатель - всегда сервер TLS.

Порт TCP с номером 6514 выделен для использования по умолчанию при передаче сообщений syslog через TLS в соответствии с данным документом.

4.2. Инициирование

Транспортному отправителю следует инициировать соединение с транспортным получателем, а затем передать TLS Client Hello для начала согласования TLS. После завершения согласования TLS транспортный отправитель **может** передать первое сообщение MAY.

TLS обычно использует сертификаты [RFC5280] для аутентификации партнёров. Разработчики **должны** поддерживать TLS 1.2 [RFC5246] и **требуется** также поддержка обязательного для реализации шифра TLS_RSA_WITH_AES_128_CBC_SHA. Предполагается применимость данного документа для будущих версий TLS и в таких случаях **должны** поддерживаться обязательные для реализации в соответствующей версии шифры.

4.2.1. Проверка подлинности на основе сертификатов

Транспортный отправитель syslog (клиент TLS) и транспортный получатель syslog (сервер TLS) **должны** поддерживать аутентификацию на основе сертификатов. Это включает проверку самого сертификата и наличия у партнёра соответствующего секретного ключа. Последняя часть выполняется TLS. Для обеспечения взаимодействия между клиентами и серверами **нужно** реализовать перечисленные ниже методы проверки приемлемости сертификатов.

- Проверка пути сертификации. Партнёр TLS имеет одну или множество доверенных привязок (обычно сертификаты корневых УЦ[1]), которые позволяют ему проверить связь между именем субъекта и открытым ключом. Нужны дополнительные правила для проверки полномочий транспортного отправителя и получателя syslog (т. е., проверки наличия полномочий у указанного именем субъекта), которые описаны в разделе 5. Проверка пути сертификации выполняется в соответствии с определением [RFC5280]. Этот метод полезен при наличии инфраструктуры открытых ключей (PKI[2]).

- Соответствие конечного элемента сертификата. В конфигурации транспортного отправителя и получателя имеется информация, требуемая для идентификации действительных сертификатов его уполномоченных партнёров. Сертификаты конечных элементов могут быть самоподписанными и в этом случае проверка пути сертификации не требуется. Реализации **должны** поддерживать отпечатки сертификатов (параграф 4.2.2) и **могут** разрешать другие форматы сертификатов конечных элементов типа сертификатов в DER-представлении. Этот метод служит дополнением к PKI, которое проще в развёртывании и обеспечивает достаточный уровень защиты.

Реализации транспортных отправителей и получателей **должны** обеспечивать средства генерации ключевых пар и самоподписанных сертификатов для случаев, когда такие пары и сертификаты недоступны с использованием иных механизмов.

Транспортным получателям и отправителям **следует** поддерживать механизмы для записи сертификатов конечных элементов с целью их сопоставления с принятыми или переданными данными.

4.2.2. Отпечатки сертификатов

Реализации клиента и сервера **должны** делать отпечатки своих сертификатов (certificate fingerprint) доступными через интерфейс управления. Метки для алгоритмов берутся из текстовых имён хэш-функций, определённых в реестре IANA Hash Function Textual Names, выделенном в [RFC4572].

Механизм генерации отпечатков заключается в том, что берётся хэш сертификата в DER-представлении с использованием криптостойкому алгоритма и результат преобразуется в разделённые двоеточиями шестнадцатеричные байты, каждый из которых представлен двумя символами ASCII в верхнем регистре. Когда значение отпечатка отображается или задаётся в конфигурации перед ним добавляется метка ASCII для хэш-функции, за которой следует двоеточие. Реализации **должны** поддерживать SHA-1 в качестве алгоритма хэширования и использовать для его идентификации метку sha-1. Размер хэш-значения SHA-1 составляет 20 байтов, а соответствующий отпечаток будет содержать 65 символов. Пример такого отпечатка приведён ниже.

```
sha-1:E1:2D:53:2B:7C:6B:8A:29:A2:76:C8:64:36:0B:08:4B:7A:F1:9E:9D
```

Для проверки хэш-значение извлекается из отпечатка и сравнивается с хэш-значением, рассчитанным для полученного сертификата.

4.2.3. Криптографический уровень

Приложения syslog **следует** реализовать так, чтобы администраторы имели возможность на уровне локальной политики выбирать желаемый криптографический уровень и опции проверки подлинности.

TLS позволяет восстанавливать предшествующую сессию TLS или использовать другую активную сессию при запросе на организацию нового сеанса. Это позволяет избавиться от издержек, связанных с полным согласованием TLS. Для запрошенной сессии снова используются параметры защиты восстанавливаемого сеанса. **Следует** проверять соответствие параметров защиты восстанавливаемой сессии требованиям защиты для запрошенной сессии.

[1] Удостоверяющий центр - CA (certification authority). *Прим. перев.*
[2] Public Key Infrastructure.

4.3. Передача данных

Все сообщения syslog **должны** передаваться как прикладные данные TLS (application data). Возможно помещать множество сообщений syslog в одну запись TLS или разделять одно сообщение syslog для передачи в нескольких записях TLS. Прикладные данные определяются приведённым ниже выражением ABNF [RFC5234].

```
APPLICATION-DATA = 1*SYSLOG-FRAME
SYSLOG-FRAME = MSG-LEN SP SYSLOG-MSG
MSG-LEN = NONZERO-DIGIT *DIGIT
SP = %d32
NONZERO-DIGIT = %d49-57
DIGIT = %d48 / NONZERO-DIGIT
SYSLOG-MSG определено в протоколе syslog [RFC5424].
```

4.3.1. Размер сообщения

Размер сообщения представляет собой значение счётчика октетов SYSLOG-MSG в SYSLOG-FRAME. Транспортный получатель **должен** использовать размер сообщения для определения его границы. Верхнего предела для размера сообщений не задаётся. Однако для обеспечения взаимодействия данная спецификация указывает, что транспортный получатель должен быть способен обрабатывать сообщения размером до 2048 октетов, включительно. Транспортным получателям **следует** поддерживать обработку сообщений размером до 8192 октетов, включительно.

4.4. Закрытие сессий

Транспортный отправитель **должен** закрывать соответствующее соединение TLS, если через него больше не планируется доставка сообщений syslog. Он **должен** передать сигнал TLS close_notify перед закрытием соединения. Транспортный отправитель (клиент TLS) **может** выбрать отказ от ожидания сигнала close_notify от транспортного получателя и просто закрыть соединение, что приводит к неполному закрытию на стороне транспортного получателя (сервер TLS). После того, как транспортный отправитель получит сигнал close_от транспортного получателя, он **должен** ответить сигналом close_notify, если у него ещё нет информации о том, что соединение уже закрыто транспортным отправителем (например, закрытие соединения указал протокол TCP).

Когда через соединение в течение продолжительного времени (интервал определяется приложением) не поступает сообщений syslog, транспортный получатель **может** закрыть соединение. Перед этим транспортный получатель (сервер TLS) **должен** предпринять попытку обмена сигналами close_notify с транспортным отправителем. Транспортные получатели, не готовые принимать никаких данных, **могут** закрыть соединение после отправки сигнала close_notify, что приводит к неполному закрытию соединения на стороне транспортного отправителя.

5. Правила безопасности

В разных средах требования безопасности различаются и, следовательно, могут использоваться разные правила. В этом разделе рассмотрены некоторые правила безопасности, которые могут применяться транспортными получателями и транспортными отправителями syslog. Правила безопасности описывают требования по проверки подлинности и полномочий. Список рассмотренных в этом разделе правил не является исчерпывающим и приложения **могут** реализовать другие правила.

Если партнёр не соответствует требованиям политики безопасности, согласование TLS **должно** прерываться с подобающим сигналом TLS.

5.1. Проверка полномочий на основе сертификата конечного элемента

В простейшем случае конфигурация транспортных отправителей и получателей включает данные, требуемые для идентификации приемлемых сертификатов своих уполномоченных партнёров.

Реализации **должны** поддерживать указание уполномоченных партнёров. с использованием отпечатков сертификатов, как описано в параграфах 4.2.1 и 4.2.2.

5.2. Проверки полномочий по имени субъекта

Реализации **должны** поддерживать проверку пути сертификации [RFC5280]. Кроме того, они **должны** поддерживать указание уполномоченных партнёров. с использованием локально заданных имён хостов и проверку соответствия имён, как описано ниже.

- Реализации **должны** поддерживать проверку локально заданных имён хостов значениям dNSName в полях расширения subjectAltName, **следует** также поддерживать проверку соответствия имени общей части отличительного имени субъекта.
- Символ-шаблон * (ASCII 42) разрешается использовать в поле dNSName расширения subjectAltName (и общем имени, если оно служит для сохранения имени хоста), но лишь в самой левой (наименее значимой) метке DNS в данном значении. Этому шаблону соответствует любая первая слева метка DNS в имени сервера. Т. е., субъект *.example.com соответствует именам сервером a.example.com и b.example.com, но не соответствует example.com и a.b.example.com. Реализации **должны** поддерживать шаблоны в сертификатах, как указано выше, но **могут** включать конфигурационную опцию для запрета этого.
- Локально заданные имена могут включать символы-шаблоны, соответствующие диапазону значений. Тип поддерживаемых шаблонов **может** быть более гибким, нежели разрешается в именах субъектов для обеспечения возможности поддержки разных правил для различных сред. Например, правило может разрешать проверку полномочий на основе «доверенного корня» (trust-root-based), где все свидетельства, выпущенные конкретным УЦ (CA), считаются полномочными.

- Если локально заданные имена являются национальными доменными именами, соответствующие требованиям реализации **должны** преобразовывать такие имена в формат ACE[1] для сравнения в соответствии с правилами раздела 7 в [RFC5280].

- Реализации **могут** поддерживать сопоставление заданных локально адресов IP со значениями iPAddress в расширении subjectAltName. В этос случае заданные локально адреса IP преобразуются в строки октетов, как указано в параграфе 4.2.1.6 [RFC5280]. Полученная строка октетов проверяется на совпадение со значением iPAddress в расширении subjectAltName.

5.3. Неаутентифицированный транспортный отправитель

В некоторых средах подлинность данных syslog не важна или проверяется иными средствами и транспортный получатель может воспринимать данные от любого транспортного отправителя. Для этого транспортный получатель может просто пропустить проверку подлинности транспортного отправителя (не запрашивая аутентификацию в TLS или принимая любые сертификаты). В таких случаях транспортный получатель является аутентифицированным и полномочным, однако такая политика не обеспечивает защиты от угроз маскирования транспортных отправителей, описанного в разделе 2. По этой причине использование такой политики **не рекомендуется**.

5.4. Неаутентифицированный транспортный получатель

В некоторых средах конфиденциальность данных syslog не важна и сообщения можно отправлять любому транспортному получателю. Для этого транспортный отправитель может пропустить проверку подлинности транспортного получателя (воспринимая любой сертификат). Хотя такая политика проверяет подлинность и полномочия транспортного отправителя, она не обеспечивает защиты от угроз маскирования транспортного получателя, описанных в разделе 2, и переданные данные остаются уязвимыми для раскрытия и изменения. По этой причине использование такой политики в общем случае **не рекомендуется**.

5.5. Неаутентифицированный транспортный получатель и отправитель

В средах, где безопасность совсем не важна, проверка подлинности (параграфы 5.3 и 5.4) может быть пропущена для транспортного получателя и транспортного отправителя. Такая политика не защищает от угроз, описанных в разделе 2 и по этой причине **не рекомендуется**.

6. Вопросы безопасности

В этом разделе описаны проблемы безопасности, дополняющие рассмотренные в [RFC5246].

6.1. Правила проверки подлинности и полномочий

В разделе 5 рассмотрены разные правила безопасности, которые могут применяться. Отмеченные в разделе 2 угрозы можно преодолеть лишь в том случае, когда транспортный отправитель и транспортный получатель подобающим образом проверяются на предмет подлинности и полномочий, как описано в параграфах 5.1 и 5.2. Такую политику безопасности **рекомендуется** устанавливать по умолчанию.

Если транспортный получатель не проверяет подлинность транспортного отправителя, он может принять данные от атакующего. Если не используется иных способов проверки подлинности источника данных, эти данные следует считать недостоверными. Особенно важно это в случаях, когда данные syslog служат для обнаружения и реагирования на инциденты безопасности. Транспортный получатель может также повысить свою уязвимость для атакам на отказ служб, неоправданного расхода ресурсов и других угроз, если не будет проверять подлинность транспортных отправителей. Поскольку такая конфигурация повышает уровень уязвимости, использовать её **не рекомендуется**.

Если транспортный отправитель не проверяет подлинность транспортного получателя syslog, он может передать свои данные злоумышленнику. Это может привести к раскрытию конфиденциальной информации из системных журналов, которая поможет атакующему и приведёт к дополнительному риску для системы. Если транспортный отправитель работает в таком режиме, ему **следует** ограничиваться передачей данных, не имеющих ценности для атакующих. Достичь этого на практике очень сложно, поэтому такие конфигурации использовать **не рекомендуется**.

Отказ от проверки подлинности и полномочий на обеих сторонах открывает их для атак MITM, маскировки и других типов, которые могут нарушить целостность и конфиденциальность данных. Такая конфигурация **не рекомендуется**.

6.2. Проверка имён

Политика проверки подлинности субъекта сертификата требует сравнения имени субъекта с заданными локально именами. Получение этих имён иными путями (типа запросов DNS) обычно неприемлема, поскольку открывает другие уязвимости защиты.

6.3. Надёжность

Следует отметить, что заданный в этом документе транспорт syslog не использует подтверждений на прикладном уровне. TCP использует повтор передачи для предотвращения некоторых типов потери данных, однако при разрыве соединения TCP (или сессии TLS) по какой-либо причине (или закрытия транспортным получателем), транспортный отправитель не всегда будет знать о том, какие сообщения были успешно доставлены приложению syslog на другой стороне.

7. Согласование с IANA

7.1. Номер порта

Агентство IANA выделило порт TCP с номером 6514 и именем syslog-tls из диапазона Registered Port Numbers. Этот порт используется по умолчанию для передачи сообщений syslog через TLS, как определено в этом документе.

[1]ASCII Compatible Encoding - совместимое с ASCII представление.

8. Благодарности

Авторы благодарят Eric Rescorla, Rainer Gerhards, Tom Petch, Anton Okmianski, Balazs Scheidler, Bert Wijnen, Martin Schuette, Chris Lonvick и членов рабочей группы syslog за их участие в дискуссиях. Авторы также признательны Balazs Scheidler, Tom Petch и другим людям за их информацию об угрозах для syslog. Авторы благодарят David Harrington за подробный анализ содержимого и грамматики документа, а также Pasi Eronen за его вклад в разделы по аутентификации и проверке полномочий.

9. Литература

9.1. Нормативные документы

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

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC5424] Gerhards, R., "The Syslog Protocol", RFC 5424, March 2009.

9.2. Дополнительная литература

[RFC4572] Lennox, J., "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)", RFC 4572, July 2006.

[SYS-SIGN] Kelsey, J., "Signed syslog Messages", Work in Progress[1], October 2007.

Адреса авторов

Fuyou Miao (редактор)

Huawei Technologies

No. 3, Xinxi Rd

Shangdi Information Industry Base

Haidian District, Beijing 100085

P. R. China

Phone: +86 10 8288 2008

EMail: miaofy@huawei.com

URI: www.huawei.com

Yuzhi Ma (редактор)

Huawei Technologies

No. 3, Xinxi Rd

Shangdi Information Industry Base

Haidian District, Beijing 100085

P. R. China

Phone: +86 10 8288 2008

EMail: myz@huawei.com

URI: www.huawei.com

Joseph Salowey (редактор)

Cisco Systems, Inc.

2901 3rd. Ave

Seattle, WA 98121

USA

EMail: jsalowey@cisco.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

[1] Работа опубликована в RFC 5848. *Прим. перев.*