Internet Engineering Task Force (IETF)
Request for Comments: 8164
Category: Experimental
ISSN: 2070-1721

M. Nottingham

M. Thomson
Mozilla

May 2017

Подходящая защита для HTTP/2

Opportunistic Security for HTTP/2

Аннотация

В этом документе описано, как можно обеспечить доступ к http URI с использованием защищённого транспорта TLS[1] и HTTP/2 для подавления всеобъемлющего мониторинга. Этот механизм не является заменой https URI и уязвим для активных атак.

Статус документа

Документ не является спецификацией проекта стандарта Internet и публикуется для проверки, экспериментальной реализации и оценки протокола.

Документ определяет экспериментальный протокол (Experimental Protocol) для сообщества Internet. Документ является результатом работы IETF[2] и представляет собой согласованное мнение сообщества IETF. Документ был вынесен на публичное рассмотрение и одобрен для публикации IESG[3]. Не все одобренные IESG документы претендуют на статус Internet Standard (см. раздел 2 в RFC 7841).

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc8164.

Оглавление

1. Введение

Документ описывает применение дополнительных служб HTTP [RFC7838] для отвязывания схемы URI от использования и настройки шифрования на нижележащих уровнях. Он обеспечивает возможность доступа к http URI [RFC7230] с использованием HTTP/2 и TLS [RFC5246] с Opportunistic Security [RFC7435].

В этом документе описана модель, посредством которой сайты могут обслуживать http URI через TLS, избегая проблемы обслуживания «смешанного содержимого (Mixed Content), описанной в [W3C.CR-mixed-content-20160802], с сохранением защиты от пассивных атак.

[1]Transport Layer Security - защита транспортного уровня.
[2]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[3]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

Модель «подходящей (уместной) защиты» (OS[1]) не обеспечивает таких же гарантий, как использование TLS с https URI, поскольку она уязвима к активным атакам, и не меняет контекста защиты соединения. Обычно пользователи просто не будут замечать её применение (не будет значка блокировки - lock icon).

1.1. Цели

Непосредственной целью является повышение устойчивости HTTP к пассивному мониторингу [RFC7258].

Другой (важной) целью является обеспечение простоты реализации, развёртывания и эксплуатации. Предполагается, что этот механизм будет оказывать минимальное влияние на производительность, требуя от администраторов лишь тривиальных действий.

Препятствие активным атакам (типа MITM[2]) не входит в задачи этой спецификации. Кроме того, данная спецификация не рассматривается в качестве замены или дополнения https, поскольку модель https обеспечивает защиту от пассивных и активных атак, а также включает более строгую модель защиты на большинстве клиентов.

1.2. 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 должны интерпретироваться в соответствии с [RFC2119].

2. Использование HTTP URI «поверх» TLS

Сервер-источник, поддерживающий преобразование http URI, может указать поддержку данной спецификации, путём анонсирования дополнительных услуг [RFC7838] для идентификатора протокола, который использует TLS (например, h2 [RFC7540]). Такой протокол **должен** включать явную индикацию схемы для ресурса. Это исключает HTTP/1.1 - клиентам HTTP/1.1 запрещено включать абсолютную форму URI в запросы к серверам-источникам (см. параграф 5.3.1 в [RFC7230]).

Клиент, получивший такой анонс, **может** делать будущие запросы к соответствующему источнику [RFC6454] с учётом этого сервиса (как указано в [RFC7838]), при условии выбора дополнительной услуги в соответствии с параграфом 2.1.

Клиент, которому важнее защита от пассивных атак, нежели производительность, может выбрать отказ от запросов, пока не станет доступным шифрованное соединение. Однако, если такое соединение организовать не удастся, клиент может возобновить использование открытого соединения.

Клиент может также явно проверить анонс дополнительных услуг, передавая запрос, не содержащий конфиденциальной информации (или содержащий немного таких данных) с использованием метода OPTIONS. Аналогично, клиенты, имеющие информацию о дополнительных услугах, могут сделать такой запрос до завершения срока действия этой информации, чтобы минимизировать возможные задержки.

Клиентские сертификаты не имеют смысла для URL в схеме http, следовательно, клиентам, организующим новые соединения TLS с дополнительными службами в соответствии с данной спецификацией, **недопустимо** представлять эти сертификаты. Серверы, которые поддерживают ресурсы https на том же порту, могут запросить сертификат в процессе согласования TLS, но им **недопустимо** прерывать согласование, если клиент не представил сертификат.

2.1. Выбор дополнительного сервера

По разным причинам сервер может перепутать в запрашиваемом URL схемы http и https (см. параграф 4.4). Для гарантии того, что дополнительные службы будут предлагаться при обработке http URL с использованием TLS, клиенты должны выполнять дополнительные проверки до отправки запросов http.

Клиентам **недопустимо** передавать запросы http через защищённые соединения, пока выбранный дополнительный сервис не представил корректный сертификат источника, как определено в [RFC2818]. Использование аутентифицированного дополнительного сервиса обеспечивает «разумные гарантии» для целей [RFC7838]. В дополнение к аутентификации сервера клиент **должен** иметь действительный отклик http-opportunistic от источника (как указано в параграфе 2.3), полученный с использованием аутентифицированного соединения. Исключение для последнего правила делается для запросов http-opportunistic от общеизвестных URI.

Предположим, например, что запрос выполняется через соединение TLS, которое аутентифицировано для этого источника. В этом случае можно передать запросы и отклики для источников http://www.example.com и http://example.com через защищённое соединение.

```
HEADERS
  + END_STREAM
  + END_HEADERS
    :method = GET
    :scheme = http
    :authority = example.com
    :path = /.well-known/http-opportunistic
HEADERS
    :status = 200
    content-type = application/json
DATA
  + END_STREAM
[ "http://www.example.com", "http://example.com" ]
```

В этом документе для удобства указывается несколько источников. Только запрос, выполненный для источника (через аутентифицированное соединение) может использоваться для получения ресурса http-opportunistic от этого источника. Таким образом, для нашего примера запрос к http://example.com не позволяет предполагать представления ресурса http-opportunistic также для http://www.example.com.

[1]Opportunistic Security.
[2]Man-in-the-middle - перехват данных в возможностью их изменения при участии человека.

2.2. Взаимодействие с https URI

Клиентам **недопустимо** передавать запросы http и https через одно соединение. Аналогично, клиентам **недопустимо** передавать через одно соединение запросы http для разных источников.

2.3. Общеизвестные http-opportunistic URI

Данная спецификация определяет общеизвестные http-opportunistic URI [RFC5785]. Клиент может считать, что у него имеется приемлемый отклик http-opportunistic для данного источника, при выполнении перечисленных ниже условий.

- Клиент запросил общеизвестный URI у источника через аутентифицированное соединение и получил отклик с кодом 200 (OK);
- этот отклик является свежим [RFC7234] (возможно через повторную проверку [RFC7232]);
- отклик имеет тип среды application/json;
- данные отклика при разборе как JSON [RFC7159] содержат массив в качестве корня;
- массив содержит строку, которая с учётом регистра посимвольно совпадает с запрашиваемым источником при последовательном представлении в кодировке Unicode, как описано в параграфе 6.1 [RFC6454].

Клиент **может** трактовать ресурс http-opportunistic, как неприемлемый, если его значения отличны от строк.

Этот документ не определяет семантики ресурсов http-opportunistic на источниках https и в тех случаях, когда ресурс содержит источники https.

Разрешение клиентам кэшировать ресурс http-opportunistic означает, что все дополнительные службы должны быть способны отвечать на запросы для ресурсов http. Клиентам разрешено использовать использовать дополнительный сервис без «приобретения» ресурса http-opportunistic от этого сервиса.

Клиентам **недопустимо** использовать кэшированную копию ресурса http-opportunistic, который был обретён (или заново проверен) через соединение без аутентификации. Во избежание возможных ошибок клиент может запросить или проверить заново ресурс http-opportunistic перед использованием любого соединения с дополнительным сервисом.

Клиенты, использующие кэшированные отклики http-opportunistic, **должны** убедиться в том, что их кэш не содержит откликов, полученных через соединения без аутентификации. Повторная проверка неаутентифицированного отклика с использованием аутентифицированного соединения не гарантирует целостности отклика.

3. Согласование с IANA

Данная спецификация регистрирует перечисленные ниже общеизвестные (well-known) URI [RFC5785]:

- URI Suffix: http-opportunistic
- Change Controller: IETF
- Specification Document(s): Section 2.3 of RFC 8164
- Related Information:

4. Вопросы безопасности

4.1. Индикаторы защиты

Пользовательским агентам **недопустимо** выводить какие-либо специальные индикаторы защищенности, когда ресурс http «обретён» с использованием TLS. В частности, **недопустимо** использовать такие же индикаторы защищенности (например, lock device), как для https.

4.2. Атаки со снижением требований

Возможны атаки, нацеленные на снижение требований при согласовании TLS.

Например, поскольку поле заголовка Alt-Svc [RFC7838] скорей всего будет присутствовать в неаутентифицированном и нешифрованном канале, оно может использоваться для атак. В простейшем варианте атакующий, который пытается принудить к организации нешифрованного соединения, может просто удалить из откликов поле заголовка Alt-Svc.

4.3. Вопросы приватности

Кэшированные дополнительные службы могут применяться для отслеживания клиентов (например, по указанному пользователем имени). Очистка кэша снижает возможности отслеживания клиентов серверами, поэтому клиенты **должны** очищать кэш информации о дополнительных службах при сбрасывании других состояний, связанных с источником (например, cookie).

4.4. Возможная путаница со схемой запроса

В реализациях и приложениях HTTP иногда применяются внешние сигналы для определения запросов, относящихся к ресурсам https (например, поиск TLS в стеке или порта 443 на сервере).

Это может быть связано с ожидаемыми ограничениями протокола (наиболее распространённые запросы HTTP/1.1 не включают явной индикации схемы URI, а ресурс может быть разработан, исходя из HTTP/1.1) или способом реализации сервера и приложения (зачастую это два разных объекта, между которыми могут использоваться самые разные интерфейсы).

Любые защитные решения, основанные на этой информации, могут быть введены в заблуждение в результате внедрения данной спецификации, поскольку она не соответствует допущению о том, что использование TLS (или порта 443) означает, что клиент обращается к HTTPS URI и работает в защищённом контексте, обеспечиваемом HTTPS.

Следовательно, разработчики и администраторы серверов должны внимательно проверить использование таких сигналов до внедрения данной спецификации.

4.5. Управление сервером

Данная спецификация требует, чтобы сервер передавал анонс дополнительных услуг в общеизвестное место для того, чтобы можно было передавать запросы HTTP через TLS. Серверам **следует** принять надлежащие меры по обеспечению контроля за содержимым общеизвестных ресурсов. Аналогично, в результате применения поля заголовка Alt-Svc для описания политики источника в целом, серверам **не следует** разрешать пользователю устанавливать или изменять значение этого заголовка.

5. Литература

5.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC 2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, DOI 10.17487/RFC2818, May 2000, <http://www.rfc-editor.org/info/rfc2818>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <http://www.rfc-editor.org/info/rfc5246>.

[RFC5785] Nottingham, M. and E. Hammer-Lahav, "Defining Well-Known Uniform Resource Identifiers (URIs)", RFC 5785, DOI 10.17487/RFC5785, April 2010, <http://www.rfc-editor.org/info/rfc5785>.

[RFC6454] Barth, A., "The Web Origin Concept", RFC 6454, DOI 10.17487/RFC6454, December 2011, <http://www.rfc-editor.org/info/rfc6454>.

[RFC7159] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March 2014, <http://www.rfc-editor.org/info/rfc7159>.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014, <http://www.rfc-editor.org/info/rfc7230>.

[RFC7232] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests", RFC 7232, DOI 10.17487/RFC7232, June 2014, <http://www.rfc-editor.org/info/rfc7232>.

[RFC7234] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Caching", RFC 7234, DOI 10.17487/RFC7234, June 2014, <http://www.rfc-editor.org/info/rfc7234>.

[RFC7540] Belshe, M., Peon, R., and M. Thomson, Ed., "Hypertext Transfer Protocol Version 2 (HTTP/2)", RFC 7540, DOI 10.17487/RFC7540, May 2015, <http://www.rfc-editor.org/info/rfc7540>.

[RFC7838] Nottingham, M., McManus, P., and J. Reschke, "HTTP Alternative Services", RFC 7838, DOI 10.17487/RFC7838, April 2016, <http://www.rfc-editor.org/info/rfc7838>.

5.2. Дополнительная литература

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC 7258, May 2014, <http://www.rfc-editor.org/info/rfc7258>.

[RFC7435] Dukhovni, V., "Opportunistic Security: Some Protection Most of the Time", RFC 7435, DOI 10.17487/RFC7435, December 2014, <http://www.rfc-editor.org/info/rfc7435>.

[W3C.CR-mixed-content-20160802] West, M., "Mixed Content", World Wide Web Consortium CR CR-mixed-content-20160802, August 2016, <https://www.w3.org/TR/2016/CR-mixed-content-20160802>.

Благодарности

Mike Bishop предоставил текст существенной части этого документа.

Спасибо Patrick McManus, Stefan Eissing, Eliot Lear, Stephen Farrell, Guy Podjarny, Stephen Ludin, Erik Nygren, Paul Hoffman, Adam Langley, Eric Rescorla, Julian Reschke, Kari Hurtta и Richard Barnes за их отклики и предложения.

Адреса авторов

Mark Nottingham
Email: mnot@mnot.net
URI: https://www.mnot.net/

Martin Thomson
Mozilla
Email: martin.thomson@gmail.com

Перевод на русский язык

Николай Малых
nmalykh@protokols.ru