Internet Engineering Task Force (IETF)
Request for Comments: 7435
Category: Informational
ISSN: 2070-1721

V. Dukhovni
Two Sigma

December 2014

# Защита, подходящая большую часть времени

**Opportunistic Security: Some Protection Most of the Time**

**Аннотация**

Этот документ определяет концепцию подходящей (уместной) защиты (OS[1]) в контексте коммуникационных протоколов. Протоколы на базе OS используют шифрование даже при недоступности аутентификации и применяют аутентификацию, когда это возможно, устраняя тем самым препятствия широкому применению шифрования в Internet.

**Статус документа**

Этот документ не является спецификацией проекта стандарта Internet и публикуется с информационными целями.

Документ является результатом работы IETF[2] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[3]. Не все одобренные IESG документы претендуют на статус Internet Standard (см. раздел 2 в RFC 5741).

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc7435.

**Авторские права**

Авторские права (Copyright (c) 2014) принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К документу применимы права и ограничения, указанные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (http://trustee.ietf.org/license-info), на момент публикации данного документа. Прочтите упомянутые документы внимательно. Фрагменты программного кода, включённые в этот документ, распространяются в соответствии с упрощённой лицензией BSD, как указано в параграфе 4.e документа IETF Trust Legal Provisions, без каких-либо гарантий (как указано в Simplified BSD License).

# Оглавление



## *1. Введение*

### 1.1. Предпосылки

Исторически протоколы защиты в Internet обеспечивали криптографическую защиту от активных и пассивных атак по принципу «все или ничего» (all or nothing). Для каждого партнёра такой протокол обеспечивает полную защиту коммуникаций или полный отказ от такой защиты. В результате операторы зачастую отключали протоколы защиты, если у пользователей возникали коммуникационные проблемы, что вело к передаче всех данных в открытом виде.

Защита от активных атак требует аутентификации. Возможность аутентифицировать каждого потенциального партнёра в сети Internet требует механизма аутентификации, который охватывает всех возможных партнёров. Ни один из стандартов IETF для аутентификации не развернут в требуемом для такой аутентификации масштабе.

Модель PKI[4] используется в браузерах для аутентификации web-серверов (её часто называют Web PKI) связана с издержками на реализацию и управление, которые ограничивают её использование. По причине наличия множества удостоверяющих центров (CA[5]), не всем из которых будет доверять каждый, взаимодействующие стороны не всегда могут согласовать взаимоприемлемый CA. Без CA, который устраивает обе стороны, аутентификация приведёт к отказу, за которым последует отказ коммуникационного протокола, для которого аутентификация обязательна. Эти

[1]Opportunistic Security.
[2]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[3]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.
[4]Public Key Infrastructure - инфраструктура открытых ключей.
[5]Certification Authority.

проблемы усугубляются эксплуатационными сложностями. Например, общей проблемой для операторов сайтов является несвоевременное обновление сертификатов с истекшим сроком действия. В интерактивных приложениях Web PKI предупреждения системы безопасности выдаются столь часто, что конечные пользователи предпочитают просто игнорировать их. Администраторы сайтов могут просто решить, что расходы на поддержку защиты не обеспечивают преимуществ и просто предоставляют своим пользователям услуги в открытом виде.

Модель TOFU[1] предполагает, что неаутентифицированный открытый ключ, полученный при первом контакте (и сохраняющийся для последующего применения), достаточно хорош для защиты будущих коммуникаций. Протокола на основе TOFU не защищают от атак, где коммуникации при первом контакте могут быть перехвачены, и требуют большей осторожности от конечного пользователя при обновлении системой своих криптографических ключей. При использовании TOFU может осложнить обнаружение различий между обычным управлением ключами и вредоносной атакой.

Модель DANE[2] [RFC6698] определяет способ распространения открытых ключей, связанных с именами DNS и может служить альтернативой для Web PKI. DANE требуется использовать в комбинации с DNSSEC [RFC4033]. На момент создания этого документа распространение DNSSEC было недостаточным для использования DANE при аутентификации потенциальных партнёров. Протоколы, запрашивающие аутентифицированные коммуникации, пока ещё не могут сделать это с помощью DANE (на момент создания этого документа).

Отсутствие глобальной системы управления ключами означает, что для многих протоколов только малую часть коммуникационных сессий можно предсказуемо аутентифицировать. Когда протокола предлагают выбор только аутентифицированных и шифрованных коммуникаций или полное отсутствие защиты, результатом является передача большей части трафика в открытом виде. Отсутствие шифрования для большей части трафика упрощает организацию всеобъемлющей слежки и снижает связанные с ней расходы (см. [RFC7258]).

Для более широкого применения шифрования аутентификацию следует сделать необязательной. Применение шифрования защитит от всеобъемлющей слежки и других пассивных атак. Даже без аутентификации шифрованные коммуникации (см. ниже) предпочтительней открытых.

## 1.2. Новые подходы

Этот документ описывает изменение подходов. До настоящего времени разработчики протоколов представляли защиту от активных и пассивных атак, как используемый по умолчанию вариант, а все, что «не дотягивало» до этого - как снижение уровня защиты и недостаток. Новое представление заключается в том, что без конкретного знания возможностей партнёра (явной настройки конфигурации или прямого запроса приложения) используемым по умолчанию вариантом считается отсутствие защиты, а все, что сверх этого является её улучшением.

Подходящая защита (Opportunistic Security или OS) определяется, как использование открытых данных в качестве базовой политики безопасности с применением по возможности согласованной и подходящей аутентификации и шифрования.

По умолчанию используется передача в открытом виде без защиты. Протокол OS не отказывается от использования защиты, которая поддерживается не всеми партнёрами. Вместо этого OS будет применять максимально доступный уровень защиты. В какой-то момент времени для конкретного приложения или протокола все, за исключением пренебрежимо малой части, партнёры смогут поддерживать шифрование. С этого момента базовый уровень защиты может быть повышен от открытой передачи до обязательного применения шифрования и только аутентификация будет выбираться из числа возможных.

Для широкого распространения протокола OS требуется возможность постепенного развёртывания. Это предполагает значительные различия возможностей защиты между разными партнёрами., возможно в течение продолжительного срока. Протоколы OS будут пытаться организовать шифрованные коммуникации, если обе стороны поддерживают шифрование, и аутентификацию, если таковая возможна. Таким образом, применение протокола OS может приводить к тому, что часть коммуникаций будет аутентифицирована и зашифрована, другая часть - зашифрована без аутентификации, а остальные будут просто открытыми. Последняя ситуация будет возникать, когда не все участники коммуникаций поддерживают шифрование (или в результате активной атаки с целью снижения уровня защиты).

При согласовании не совсем полной защиты не требуется выводить для пользователя диалоговое окно «Ваша защита может быть слабой, нажмите OK» (your security may be degraded, please click OK). Согласованный уровень защиты является лучшим из числа возможных. Даже если эта защита является не полной, она все равно будет лучше, чем традиционный выбор между «без защиты» и «коммуникационный отказ».

Протокол OS не предназначен на замену аутентифицированным и шифрованным коммуникациям, которые уже требуются для доступа к ресурсу в соответствии с политикой (т. е., из конфигурации или прямого запроса приложения) или по иным причинам. По сути, OS используется в тех случаях, когда без этого протокола данные просто передавались бы в открытом виде. Протоколы OS никогда не препятствуют выполнению явных правил безопасности. Администратор безопасности может задать правила, которые будут переопределять OS. Например, политика может требовать аутентифицированных и шифрованных коммуникаций, а не принятой по умолчанию политики защиты OS.

В этом документе термин opportunistic используется в позитивном смысле. На основе анонсированных партнёром возможностей протокол OS выбирает максимально возможный уровень защиты. Прилагательное opportunistic относится к адаптивному выбору механизмов защиты для каждого партнёра. После того, как для данного партнёра выбран уровень защиты, OS слабо отличается от других вариантов, использующих тот же набор механизмов.

В оставшейся части этого документа даны определения важных терминов, описаны принципы работы OS и приведён пример устройства OS для случая взаимодействия двух почтовых трансляторов.

[1] Trust-on-first-use - доверять при первом использовании.
[2] DNS-Based Authentication of Named Entities - основанная на DNS аутентификация именованных элементов.

# 2. Термины

***Trust on First Use (TOFU) - доверие при первом обращении***

В протоколе TOFU вызывается для восприятия и сохранения открытого ключа или свидетельства (credential), связанного с заявленным отождествлением, без аутентификации этого отождествления. Последующие коммуникации, которые аутентифицируются с использованием кэшированного ключа или свидетельства, будут защищены от MiTM-атак, если такая атака не была успешно организована во время уязвимого начального контакта. Наиболее широко распространённой формой использования TOFU является протокол SSH [RFC4251]. В качестве синонима TOFU иногда используется фраза leap of faith (скачок доверия) [RFC4949].

***Authenticated, encrypted communication - аутентифицированные, шифрованные коммуникации***

Шифрованные коммуникации, использующие метод организации сессии, в котором по крайней мере инициатор (или клиент) проверяет отождествление отвечающей стороны (или сервера). Это требуется для защиты от пассивных и активных атак. Взаимная аутентификация, при которой сервер также проверяет отождествление клиента, играют роль в смягчении активных атак, когда роли клиента и сервера меняются в течение одной сессии.

***Unauthenticated, encrypted communication - неаутентифицированные, шифрованные коммуникации***

Шифрованные коммуникации, использующие метод организации сессий без проверки отождествления партнёров. В типичной ситуации это означает, что инициатор (клиент) не проверяет отождествление отвечающей стороны (сервера), что делает возможными MiTM-атаки.

***Perfect Forward Secrecy (PFS)***

См. определение в [RFC4949].

***Man-in-the-Middle (MiTM) attack - перехват данных с возможностью их изменения при участии человека***

См. определение в [RFC4949].

***OS protocol - протокол OS***

Протокол, поддерживающий модель подходящей (уместной) защиты, описанную здесь.

# 3. Устройство OS

OS обеспечивает краткосрочное решение для борьбы с пассивными атаками за счёт устранения препятствий широкому использованию шифрования. OS предлагает путь постепенного перехода к аутентифицированным, шифрованным коммуникациям по мере внедрения подходящих технологий проверки подлинности. Основные принципы OS перечислены ниже

***Сосуществование с явными правилами***

Явные правила и политика безопасности преобладают над OS. Уместная защита никогда не подменяет и не отменяет заданных явно правил защиты. Многие приложение и типы данных слишком деликатны[1] для использования OS и в таких случаях нужно применять традиционные способы и средства защиты.

***Приоритизация коммуникаций***

Основная цель OS заключается в максимизации развёртывания. уместных средств защиты без создания препятствий при коммуникациях. Протоколы OS нужно внедрять постепенно с независимой настройкой конфигурации каждого партнёра, выполняемой его администратором или пользователем. При использовании OS коммуникационные возможности сохраняются даже в тех случаях, когда один партнёр поддерживает аутентификацию и/или шифрование, а другой не поддерживает.

***Максимальная защита коммуникаций между партнёрами. одного уровня***

Протоколы OS применяют шифрование, если оно поддерживается на обеих сторонах соединения. Протоколы OS форсируют аутентификацию партнёра, когда доступен аутентифицированный отдельный канал (out-of-band) для передачи ключей или свидетельств. В общем случае, коммуникации следует хотя бы шифровать. OS следует по возможности применять PFS для того, чтобы защитить ранее записанные шифрованные коммуникации от расшифровки даже в случае взлома или кражи долгосрочных ключей.

***Отсутствие ложной трактовки безопасности***

Неаутентифицированные шифрованные коммуникации не должны создавать у пользователей и в системных журналах неинтерактивных приложений иллюзии эквивалентности аутентифицированным шифрованным коммуникациям.

Протокол OS сначала определяет возможности партнёра, с которым он пытается взаимодействовать. Эти возможности можно обнаружить с использованием основного канала (in-band, с использованием того или иного согласования между партнёрами.) или иных путей (out-of-band, включая записи DANE, а также кэшированные ключи или свидетельства, полученные с помощью TOFU). Фаза определения возможностей может указать, что партнёр поддерживает аутентифицированные и шифрованные, неаутентифицированные и шифрованные коммуникации или просто обмен данными в открытом виде.

Шифрование применяется для снижения риска атак с пассивным мониторингом, тогда как аутентификация позволяет снизить риск активных MiTM-атак. При анонсировании возможности шифрования через незащищённый канал возможна MiTM-атака для согласования передачи в открытом виде вместо шифрования. С целью защиты от MiTM-атак для аутентификации анонсы возможностей с указанием поддержки аутентификации нужно передавать через отдельный (out-of-band) аутентифицированный канал, который сам по себе устойчив к MiTM-атакам.

Протоколы OS могут сталкиваться с трудностями, если анонсированные партнёром функции защиты приводят к отказам. Функции защиты, которые надёжно работают (при отсутствии атаки), скорее всего будут развёрнуты и включены по умолчанию. Очень важно, чтобы возможности, анонсируемые поддерживающему OS партнёру, соответствовали реальным. В противном случае системы OS будут воспринимать отказы таких служб, как активную атаку, что может приводить к коммуникационным сбоям. Это может означать дополнительную фильтрацию анонсируемых партнёром возможностей с целью сохранения только тех, которые работают достаточно надёжно. Возможности, от которых не ожидается надёжной работы в OS, следует рассматривать, как «отсутствующие» или «неопределённые».

При аутентифицированных и шифрованных коммуникациях протоколы OS могут использовать более мягкие параметры по сравнению с защитой, которую обычно принято задавать правилами. Некоторые устаревшие системы поддерживают шифрование, но используют для этого старые алгоритмы или версии протоколов. Совместимость с такими системами позволяет избежать передачи данных в открытом виде.

[1] Например, конфиденциальны. *Прим. перев.*

Для более надёжной защиты канала протокол OS может потребовать более строгих криптографических параметров при аутентификации сессии. Например, из числа разрешённых шифров для TLS[1] [RFC5246] могут быть исключены устаревшие (deprecated) алгоритмы, которые допускаются для шифрованных неаутентифицированных коммуникаций.

Протоколам OS следует создавать аутентифицированные и шифрованные соединения, когда «ожидается» аутентификация партнёра. Здесь термин «ожидается» означает определение по устойчивому к снижению уровня защиты каналу, что проверка подлинности партнёра будет работать. Устойчивые к снижению уровня защиты методы включают проверенные записи DANE DNS, имеющаяся информация TOFU об отождествлении, а также настроенная вручную конфигурация. Такое использование аутентификации является подходящим (opportunistic) в том смысле, что она выполняется на уровне сессии при наличии возможности.

При взаимодействии с партнёром, который поддерживает только шифрование (без аутентификации), любые проверки подлинности, включённые по умолчанию, должны быть отключены или настроены на «мягкое» отключение (soft-fail), чтобы избежать ненужных коммуникационных отказов или необходимости перехода к открытым данным.

Поддержка работы с открытыми данными и устаревшими алгоритмами (особенно, взломанных) служит для совместимости с развёрнутыми ранее системами. Для протоколов, основанных на OS, предпочтительно шифровать данные с использованием наиболее подходящего алгоритма из числа доступных. Протоколы OS реализуют открытую передачу и взломанные алгоритмы шифрования только для партнёров., которые не способны на иное. Желание состоит в отказе от передачи открытых данных и использования взломанных алгоритмов и для этого весьма важно исключить такую функциональность из реализаций.

## *4. Пример - TLS в SMTP*

Большинство агентов MTA[2] [RFC5598] поддерживает расширение STARTTLS [RFC3207] для ESMTP. Агенты MTA, выступающие в качестве клиентов SMTP [RFC5321], обычно используют передачу электронной почты в открытом виде. Они согласуют шифрование TLS в тех случаях, когда сервер SMTP анонсирует поддержку STARTTLS. Поскольку начальное согласование ESMTP не использует криптографической защиты, анонсы STARTTLS уязвимы к MiTM-атакам, направленным на снижение уровня защиты.

Недавние отчёты множества крупных провайдеров (например, [fb-starttls] и [goog-starttls]) показали, что основная часть электронной почты SMTP в сети Internet в настоящее время шифруется и видна тенденция к росту этого показателя.

У разных MTA, анонсирующих STARTTLS, возникают проблемы взаимодействия. Для обхода этих проблем клиенты MTA обычно возвращаются к передаче почты в открытом виде, если при согласовании или в процессе работы TLS возникают отказы. Это является разумным компромиссом, поскольку STARTTLS защищает лишь от пассивных атак. При отсутствии активной атаки отказы TLS обычно связаны с какой-либо из известных проблем взаимодействия.

Некоторые клиенты MTA с поддержкой STARTTLS прерывают согласование TLS, если аутентификация сервера MTA приводит к отказу и сразу переходят к обмену открытыми данными. Было замечено, что некоторые MTA воспринимают самоподписанные сертификаты, но отказываются принимать просроченные и также переходят к обмену открытыми данными. Такое поведение **не** согласуется с принципами OS, поскольку происходит переход к обмену открытыми данными, хотя шифрование возможно.

Защита от активных атак для SMTP описана [SMTP-DANE], где вводятся термины Opportunistic TLS и Opportunistic DANE TLS. Такой подход совместим с принципами OS, определёнными в данном документе. В режиме Opportunistic DANE TLS организуются аутентифицированные и шифрованные коммуникации с партнёрами., для которых имеется подходящая запись DANE. Для прочих партнёров. используется режим Opportunistic TLS, как и без OS.

## *5. Эксплуатационные вопросы*

При разработке протоколов OS следует минимизировать возможность отказа согласованных механизмов защиты. Протоколам OS может потребоваться снижение уровня защиты (fallback) для обхода отказов механизмов защиты, вызываемых на практике проблемами взаимодействия. Выбирать реализацию или включение механизма снижения уровня защиты следует лишь при возникновении существенных проблем в работе.

Когда согласована только защита от пассивных атак через канал, уязвимый для активных атак со снижением уровня защиты, и отказе при использовании шифрования, протокол может выбрать открытый обмен данными. Отказ при шифровании чаще является признаком проблем взаимодействия, а не активной атаки. В такой ситуации переход к обмену в открытом виде может оказаться хорошим решением. Хотя в этом случае часть трафика передаётся в открытом виде, без этого пришлось бы просить администратора или пользователя вручную обходить проблемы совместимости. Если инциденты такого типа происходят достаточно часто, может оказаться разумным административное отключение OS.

## *6. Вопросы безопасности*

OS поддерживает коммуникации с шифрованием и аутентификацией, с шифрованием без аутентификации или просто в открытом виде. Уровень защиты, обеспечиваемой взаимодействующим партнёрам не снижается при использовании OS, поскольку политика OS заключается в предложении наилучших защитных услуг на основе возможностей партнёров., а заданная явно политика имеет преимущество перед принятой по умолчанию политикой OS. OS обеспечивает преимущество по сравнению со сложившейся практикой, поскольку обеспечивает максимально возможную защиту вместо отказа от шифрования при невозможности выполнить проверку подлинности партнёра (если она не задана жёстко.

Хотя использование OS отменяется явной политикой, не связанной с OS, такая политика может оказаться менее эффективной для случаев работы с множеством партнёров. Правила без OS следует применять с осторожностью, чтобы пользователи не сочли их слишком жёсткими и просто не отключили защиту совсем.

Когда протоколы следуют модели OS, злоумышленники, участвующие во всеобъемлющем пассивном мониторинге, уже не смогут собирать все подряд и вынуждены будут более выборочно определять объекты слежки и/или

[1]Transport Layer Security - защита транспортного уровня.
[2]Message Transfer Agent - агент передачи сообщений.

организовывать более активные атаки. В дополнение к этому применение OS означает, что активные атаки, к которым вынуждены будут перейти злоумышленники, будет легче обнаружить.

Конкретные методы обнаружения и ослабления активных атак в отсутствие аутентификации выходят за рамки этого документа. Некоторые имеющиеся протоколы, которые могут поддерживать OS, могут оказаться уязвимыми к сравнительно недорогим атакам на снижение уровня защиты, организованным злоумышленниками на пути передачи данных. Однако при повсеместном использовании таких атак (например, для организации слежки) они легко обнаруживаются. Поэтому в таких случаях протоколы OS обеспечивают преимущество.

Протоколам, соответствующим модели OS, может потребоваться определение дополнительных мер для снижения возможности систематического снижения уровня защиты или повышения вероятности обнаружения таких атак. При обретении дополнительного опыта в этом направлении будущие версии данного документа или связанных с ним документов смогут дать более применимые на практике рекомендации.

# *7. Литература*

## 7.1. Нормативные документы

[RFC3207] Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security", RFC 3207, February 2002, <http://www.rfc-editor.org/info/rfc3207>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005, <http://www.rfc-editor.org/info/rfc4033>.

[RFC4251] Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Protocol Architecture", RFC 4251, January 2006, <http://www.rfc-editor.org/info/rfc4251>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007, <http://www.rfc-editor.org/info/rfc4949>.

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

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, October 2008, <http://www.rfc-editor.org/info/rfc5321>.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, August 2012, <http://www.rfc-editor.org/info/rfc6698>.

## 7.2. Дополнительная литература

[RFC5598] Crocker, D., "Internet Mail Architecture", RFC 5598, July 2009, <http://www.rfc-editor.org/info/rfc5598>.

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

[SMTP-DANE] Dukhovni, V. and W. Hardaker, "SMTP security via opportunistic DANE TLS", Work in Progress, draft-ietf-dane-smtp-with-dane-13, October 2014.

[fb-starttls] Facebook, "The Current State of SMTP STARTTLS Deployment", May 2014, <https://www.facebook.com/notes/protect-the-graph/the-current-state-of-smtp-starttls-deployment/1453015901605223>.

[goog-starttls] Google, "Safer email - Transparency Report - Google", June 2014, <https://www.google.com/transparencyreport/saferemail/>.

# *Благодарности*

Автор благодарен Dave Crocker, Peter Duchovni, Paul Hoffman, Benjamin Kaduk, Steve Kent, Scott Kitterman, Pete Resnick, Martin Thomson, Nico Williams, Paul Wouters и Stephen Farrell за множество полезных предложений и поддержку.

# *Адрес автора*

**Viktor Dukhovni**

Two Sigma

EMail: ietf-dane@dukhovni.org

**Перевод на русский язык**

Николай Малых

nmalykh@protokols.ru