УДК 004.7

Исследование проблем перехода с протокола Transport Layer Security версии 1.2 на версию 1.3

Романов Вадим Николаевич roma.vadick@yandex.ru
Молчанов Алексей Николаевич molchanov@bmstu.ru

КФ МГТУ им. Н.Э. Баумана, Калуга, Россия

В настоящее время для защиты передаваемых данных в сети используются 2 *версии криптографического протокола* Transport Layer Security (TLS): 1.2 *и* 1.3. *Цель доклада — проанализировать преимущества и недостатки обеих версий протокола, а именно используемые протоколы шифрования, протоколы аутентификации и обмена ключами, скорость и эффективность обеих версий протоколов, их уязвимости и функции, а также поддержку старых протоколов и компромисс между безопасностью и совместимостью; выявить проблемы перехода с протокола версии* 1.2 *на* 1.3, *их потенциальные причины и возможные последствия и предложить пути решения этих проблем; сделать выводы о проведенном исследовании.*

***Ключевые слова*:** *протокол* Transport Layer Security, *криптография, безопасность в сети, конфиденциальность, алгоритмы шифрования*

Протокол Transport Layer Security (TLS) играет решающую роль в обеспечении безопасности передачи данных в сети Интернет, обеспечивая защищенный канал между клиентом и сервером для организации конфиденциальности и целостности данных, а также для аутентификации сторон. По мере развития технологий и появления новых угроз безопасности, стандарты TLS постоянно совершенствуются. В настоящее время используется две версии протокола: TLS 1.2 и 1.3 [1].

TLS 1.2 был выпущен в августе 2008 г. и поддерживает протоколы шифрования AES, 3DES, RC4 и Camelia. Однако он имеет уязвимости к атакам, таким как POODLE, BEAST и CRIME. Эта версия допускает поддержку устаревших и уязвимых протоколов, чтобы обеспечить совместимость с различными клиентами [2].

TLS 1.3 был выпущен в августе 2018 г. и предлагает более надежные протоколы шифрования, такие как AES-GCM и ChaCha20-Poly1305. Уязвимости версии 1.2 были исправлены, и поддержка устаревших протоколов, таких как SSLv3, была прекращена. Эта версия акцентирует внимание на безопасность даже за счет совместимости и включает новые функции, такие как 0-RTT и поддержка HTTP/2 [2]. Полная сравнительная оценка приведена в таблице.

Таким образом, более надежным и практичным является протокол TLS версии 1.3. Переход с TLS 1.2 на 1.3 требует внимательного рассмотрения, так как это не просто обновление протокола, но и переход к новым криптографическим методам и алгоритмам.

Сравнение версий протокола TLS

Характеристика	Версия протокола	
	TLS 1.2	TLS 1.3
Релиз	Август 2008 г.	Август 2018 г.
Протоколы шифрования	AES, 3DES, RC4, Camelia	AES-GCM, ChaCha20-Poly1305 (более надежные)
Протоколы аутентификации	RSA, DSA, ECDSA	RSA, ECDSA, PSK (возможность совместного использования)
Протоколы обмена ключами	RSA, DHE, ECDHE, PSK	ECDHE, PSK, (не поддерживаются RSA и DHE)
Скорость и эффективность	Относительно ниже	Улучшена
Уязвимости	Уязвимости к атакам, включая POODLE, BEAST, CRIME	Исправлены уязвимости версии 1.2
Поддержка старых протоколов	Допускает поддержку устаревших и уязвимых протоколов	Прекращена поддержка устаревших протоколов, таких как SSLv3
Новые функции и возможности	–	Введены новые механизмы защиты, такие как 0-RTT и поддержка HTTP/2
Компромисс между безопасностью и совместимостью	Больший акцент на совместимость для обеспечения поддержки различных устаревших клиентов	Больший акцент на безопасность, даже за счет совместимости

Основными проблемами перехода являются следующие.

1. Совместимость с устаревшими клиентами и серверами:

– проблема: некоторые старые клиенты и серверы могут не поддерживать TLS 1.3, что может привести к проблемам с совместимостью и недоступности сервисов для пользователей;

– потенциальные причины: устаревшие версии операционных систем, библиотеки SSL/TLS и настраиваемые приложения могут не иметь поддержки для TLS 1.3;

– возможные последствия: необходимость обслуживания устаревших систем для обеспечения совместимости может увеличить сложность инфраструктуры и ресурсозатраты [2].

2. Интеграция с существующими системами и приложениями:

– проблема: некоторые системы и приложения могут иметь зависимости от функциональности, которая может быть нарушена при переходе на TLS 1.3;

– потенциальные причины: приложения, использующие устаревшие API или криптографические библиотеки, могут быть не совместимы с новым протоколом;

– возможные последствия: необходимость переписывания или модификации существующего кода для поддержки TLS 1.3 может быть трудоемкой и времязатратной [1].

3. Обучение и подготовка персонала:

– проблема: переход на новый протокол требует обучения персонала и ознакомления с новыми функциями и возможностями;

– потенциальные причины: сотрудники могут быть не знакомы с новыми механизмами защиты или процессами, связанными с TLS 1.3;

– возможные последствия: необходимость обучения персонала может замедлить процесс внедрения нового протокола и увеличить временные затраты.

4. Тестирование и отладка:

Проблема: переход на новый протокол требует обширного тестирования и отладки, чтобы обеспечить его стабильность и безопасность.

Потенциальные причины: внедрение нового протокола может привести к появлению новых ошибок или уязвимостей.

Возможные последствия: недостаточное тестирование и отладка могут привести к проблемам с безопасностью или непредвиденным сбоям системы [3].

Для устранения вышеперечисленных проблем могут быть приняты следующие решения.

Совместимость с устаревшими клиентами и серверами:

– обновление или замена устаревших систем и приложений, чтобы они поддерживали TLS 1.3;

– использование прокси-серверов или шлюзов для обеспечения совместимости с устаревшими клиентами.

Интеграция с существующими системами и приложениями:

– переписывание или модификация кода существующих систем и приложений для поддержки TLS 1.3;

– использование адаптеров или промежуточного слоя для обеспечения совместимости [4].

Обучение и подготовка персонала:

– проведение обучающих семинаров и тренингов для персонала по использованию и поддержке TLS 1.3;

– создание документации и руководств по внедрению и использованию нового протокола [2].

Тестирование и отладка:

– проведение обширного тестирования перед внедрением TLS 1.3 в продакшн среду;

– постепенное внедрение нового протокола с мониторингом и отладкой на каждом этапе [4].

Переход на TLS 1.3 открывает новые возможности для повышения безопасности и эффективности сетевых коммуникаций, что способствует развитию более надежных и защищенных цифровых экосистем. Однако этот процесс может столкнуться с рядом вызовов и проблем, включая совместимость с устаревшими системами, интеграцию с существующими приложениями,

обучение персонала и обширное тестирование. Путем анализа и оценки рисков организация сможет разработать наиболее эффективные стратегии перехода на TLS 1.3, минимизируя негативное воздействие на бизнес-процессы и обеспечивая максимальный уровень безопасности.

Литература

[1] Дэвис Д. *Реализация* SSL/TLS *с использованием криптографии и* PKI. URL: https://skillexperto.com/index/implementing-ssl-tls-using-cryptography-and-pki/ (дата обращения 14.03.2024).

[2] Опплигер Р. SSL *и* TLS: *Теория и практика*. URL: https://swrdfish.github.io/assets/ssl/SSLandTLSTheoryandPractice.pdf (дата обращения 14.03.2024).

[3] Ристич И. *Надежный* SSL *и* TLS. URL: https://vk.com/doc-67988210_463291776?hash=IFPUhu1Z8hCMnQHZY22cqDFQWKkMqt1oT1xYV2dpeqL&dl=swDODIx4XuWGC8usNwS (дата обращения 14.03.2024).

[4] Экрес Х., Бака П., Шаттен Д. SSL/TLS *под замком и ключом. Руководство по пониманию криптографии* SSL/TLS. URL: https://books.google.ru/books/about/SSL_TLS_Under_Lock_and_Key.html?hl=ru&id=344OEAAAQBAJ&redir_esc=y (дата обращения 14.03.2024).

Investigation of the problems of the transition from the Transport Layer Security protocol version 1.2 to version 1.3

Romanov Vadim Nikolaevich roma.vadick@yandex.ru
Molchanov Alexey Nikolaevich molchanov@bmstu.ru

Kaluga branch of BMSTU, Kaluga, Russia

Currently, 2 versions of the Transport Layer Security (TLS) cryptographic protocol are used to protect transmitted data on the network: 1.2 and 1.3. The purpose of the report is to analyze the advantages and disadvantages of both versions of the protocol, namely: encryption protocols used, authentication and key exchange protocols, speed and efficiency of both versions of protocols, their vulnerabilities and functions, as well as support for old protocols and a compromise between security and compatibility; identify problems with the transition from protocol version 1.2 to 1.3, their potential causes and possible consequences and suggest ways to solve these problems; draw conclusions about the study.

Keywords: Transport Layer Security protocol, cryptography, security in the network, confidentiality, encryption algorithms