УДК 004.056.5

Недвига Константин Сергеевич, студент,
Донской государственный технический университет
Nedviga Konstantin Sergeevich, student,
Don State Technical University

Головягин Алексей Дмитриевич, студент,
Донской государственный технический университет
Golovyagin Alexey Dmitrievich, student,
Don State Technical University

Шевчук Петр Сергеевич,
доктор технических наук, профессор,
профессор кафедры «Информационная безопасность
в вычислительных системах и сетях»,
Донской государственный технический университет
Shevchuk Petr Sergeevich,
Doctor of Technical Sciences, Professor,
Professor, Department of Information Security
in Computing Systems and Networks,
Don State Technical University

АНАЛИЗ УЯЗВИМОСТЕЙ ПРОТОКОЛА TLS 1.3 И ОЦЕНКА ЭФФЕКТИВНОСТИ МЕР ПРОТИВОДЕЙСТВИЯ АТАКАМ ПОНИЖЕНИЯ ВЕРСИИ
VULNERABILITY ANALYSIS OF THE TLS 1.3 PROTOCOL AND EVALUATION OF DOWNGRADE-ATTACK COUNTERMEASURE EFFECTIVENESS

Аннотация. В работе проанализированы уязвимости протокола TLS 1.3, связанные с атаками понижения версии, и оценена эффективность встроенных мер противодействия. Рассмотрен механизм согласования версии на основе расширения supported_versions и защитный контроль downgrade sentinel в поле ServerHello.random. Предложена модель остаточного риска, учитывающая коэффициент покрытия защитных механизмов. Показано, что эффективность защиты определяется не столько самим протоколом, сколько корректностью его реализации и настройкой допустимых версий на оконечных узлах.

Abstract. The paper analyses the vulnerabilities of the TLS 1.3 protocol related to downgrade attacks and evaluates the effectiveness of its built-in countermeasures. The version negotiation mechanism based on the supported_versions extension and the downgrade-sentinel control in the ServerHello.random field are considered. A residual-risk model that accounts for the coverage coefficient of the protective mechanisms is proposed. It is shown that the effectiveness of protection depends not so much on the protocol itself as on the correctness of its implementation and on the configuration of the permitted versions at the endpoints.

Ключевые слова: TLS 1.3, атака понижения версии, downgrade sentinel, supported_versions, MITM, оценка эффективности.

Keywords: TLS 1.3, downgrade attack, downgrade sentinel, supported_versions, MITM, effectiveness evaluation.

Введение.

Протокол TLS (Transport Layer Security) является основным средством защиты трафика в информационно-телекоммуникационных сетях, обеспечивая конфиденциальность,

целостность и аутентификацию сторон. Общие принципы криптографической защиты подробно изложены в специальной литературе [6, 7]. Версия TLS 1.3, стандартизованная в документе RFC 8446, существенно упростила процедуру установления соединения и исключила ряд устаревших криптографических примитивов [1]. Тем не менее сохраняется класс угроз, связанных с атаками понижения версии (downgrade attacks), при которых активный нарушитель вынуждает стороны согласовать более старую и менее защищённую версию протокола. Именно этот механизм лежал в основе известных атак FREAK, Logjam и POODLE, эксплуатировавших слабости ранних версий SSL/TLS [4, 5].

Цель работы – проанализировать уязвимости TLS 1.3 в части атак понижения версии и оценить эффективность встроенных мер противодействия применительно к различным сценариям развёртывания.

Согласование версии в TLS 1.3.

В отличие от предшествующих версий, где номер версии передавался непосредственно в поле client_version сообщения ClientHello, в TLS 1.3 согласование версии вынесено в отдельное расширение supported_versions, а поле legacy_version зафиксировано значением 0x0303 (соответствующим TLS 1.2) [2] для совместимости с промежуточными узлами [1]. Клиент перечисляет в расширении поддерживаемые версии, а сервер выбирает наибольшую из общих. Такое разделение позволило развернуть TLS 1.3 в существующей инфраструктуре, однако одновременно создало точку воздействия: активный нарушитель, находящийся между клиентом и сервером (модель «человек посередине», MITM), может удалить или изменить расширение supported_versions, вынудив стороны согласовать TLS 1.2 или более раннюю версию.

Атака понижения версии.

Обобщённая схема атаки понижения версии и механизма её обнаружения приведена на рисунке 1. Нарушитель перехватывает сообщение ClientHello и удаляет из него расширение supported_versions. Сервер, не обнаружив признаков поддержки TLS 1.3, отвечает сообщением ServerHello с выбранной версией TLS 1.2. В результате, несмотря на то что обе стороны поддерживают TLS 1.3, устанавливается соединение по устаревшему протоколу, к которому применимы ранее известные атаки.

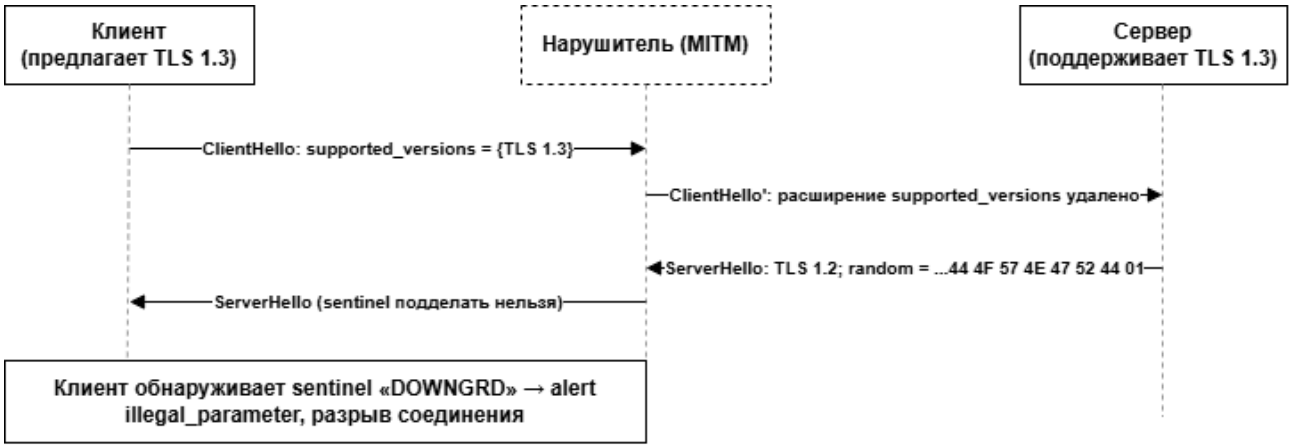

Рисунок 1. Атака понижения версии TLS и механизм её обнаружения

Встроенные меры противодействия.

Основным механизмом защиты TLS 1.3 от понижения версии служит контрольное значение (downgrade sentinel), размещаемое сервером в последних восьми байтах поля ServerHello.random [1]. Если сервер, поддерживающий TLS 1.3, согласует TLS 1.2, он обязан установить эти байты равными последовательности 44 4F 57 4E 47 52 44 01 (первые семь байт

кодируют строку «DOWNGRD»); при согласовании TLS 1.1 или ниже используется последовательность 44 4F 57 4E 47 52 44 00. Клиент, предлагавший TLS 1.3 и получивший ответ с версией TLS 1.2 или ниже, обязан проверить последние восемь байт и при совпадении с любым из указанных значений прервать рукопожатие с оповещением illegal_parameter.

Стойкость данного механизма обеспечивается тем, что значение ServerHello.random входит в подписываемые в ходе рукопожатия данные (в TLS 1.2 подпись сервера в сообщении ServerKeyExchange покрывает оба случайных значения). Поэтому активный нарушитель не может удалить контрольную последовательность, не нарушив проверку подписи, и попытка понижения версии становится обнаруживаемой. Дополнительной защитой служит завершающее сообщение Finished, содержащее имитовставку по всему транскрипту рукопожатия. Для сценариев повторного соединения с откатом версии применяется также сигнальный набор шифров TLS_FALLBACK_SCSV, определённый в RFC 7507 [3].

Вероятность случайного совпадения последних восьми байт случайного поля с фиксированной контрольной последовательностью пренебрежимо мала:

$$P_{совп} = 2^{-64} \approx 5{,}4 \cdot 10^{-20} \quad (1)$$

что позволяет считать ложные срабатывания механизма практически невозможными.

Уязвимости и остаточные риски.

Анализ показывает, что рассмотренный механизм защищает соединение лишь при выполнении ряда условий. Во-первых, контрольная последовательность выставляется и проверяется только тогда, когда обе стороны поддерживают TLS 1.3; если сервер действительно поддерживает лишь TLS 1.2, понижение версии является штатным и не может быть отличено от атаки, а итоговая защищённость определяется стойкостью TLS 1.2. Во-вторых, эффективность контроля целиком зависит от корректности реализации на стороне клиента: если клиент не проверяет sentinel, откат остаётся незамеченным. Такой дефект был выявлен, в частности, в библиотеке utls версий до 1.7.0, где клиент принимал понижение версии без проверки контрольного значения. В-третьих, устаревшие промежуточные узлы, некорректно обрабатывающие согласование версии, способны непреднамеренно инициировать откат. Наконец, если оконечный узел допускает использование TLS 1.0 или SSL 3.0, сохраняется возможность отката к заведомо уязвимым версиям. Отдельным классом угроз TLS 1.3, не относящимся напрямую к понижению версии, являются атаки повторного воспроизведения ранних данных (0-RTT), которые следует учитывать при проектировании защиты.

Оценка эффективности мер противодействия.

Для количественной оценки введём модель остаточного риска. Остаточный риск понижения версии определяется вероятностью попытки атаки, долей непокрытых защитой сценариев и величиной возможного ущерба:

$$R_{ост} = P_a \cdot (1 - K_з) \cdot У \quad (2)$$

где Ра – вероятность попытки атаки, Кз – коэффициент покрытия защитных механизмов, У – величина ущерба. При совместном применении нескольких независимых механизмов (проверка sentinel, SCSV, отключение устаревших версий) суммарный коэффициент покрытия определяется выражением:

$$K_з = 1 - \prod (1 - k_i) \quad (3)$$

где ki – коэффициент покрытия i-го механизма. Из выражения (3) следует, что эшелонирование мер повышает суммарное покрытие: даже при отказе одного механизма остальные снижают остаточный риск. Качественная оценка остаточного риска для характерных сценариев приведена в таблице 1, а её наглядное представление – на рисунке 2. Приведённые значения носят экспертный, иллюстративный характер и подлежат уточнению по результатам испытаний конкретной конфигурации.

Таблица 1

Эффективность мер противодействия по сценариям развёртывания

Сценарий	**Механизм защиты (sentinel / SCSV)**	**Итог**
Клиент и сервер поддерживают TLS 1.3, sentinel проверяется	срабатывает	атака обнаруживается, соединение разрывается
Клиент не проверяет sentinel (ошибка реализации)	не срабатывает	откат до TLS 1.2 не обнаруживается
Сервер поддерживает только TLS 1.2	sentinel не выставляется, откат легитимен	версия понижается штатно; риск определяется стойкостью TLS 1.2
Клиент допускает TLS 1.0 / SSL 3.0	зависит от узлов, защита ослаблена	возможен откат к уязвимым версиям (POODLE и др.)
Повторное соединение с откатом, задействован TLS_FALLBACK_SCSV	срабатывает (SCSV)	сервер обрывает некорректный откат

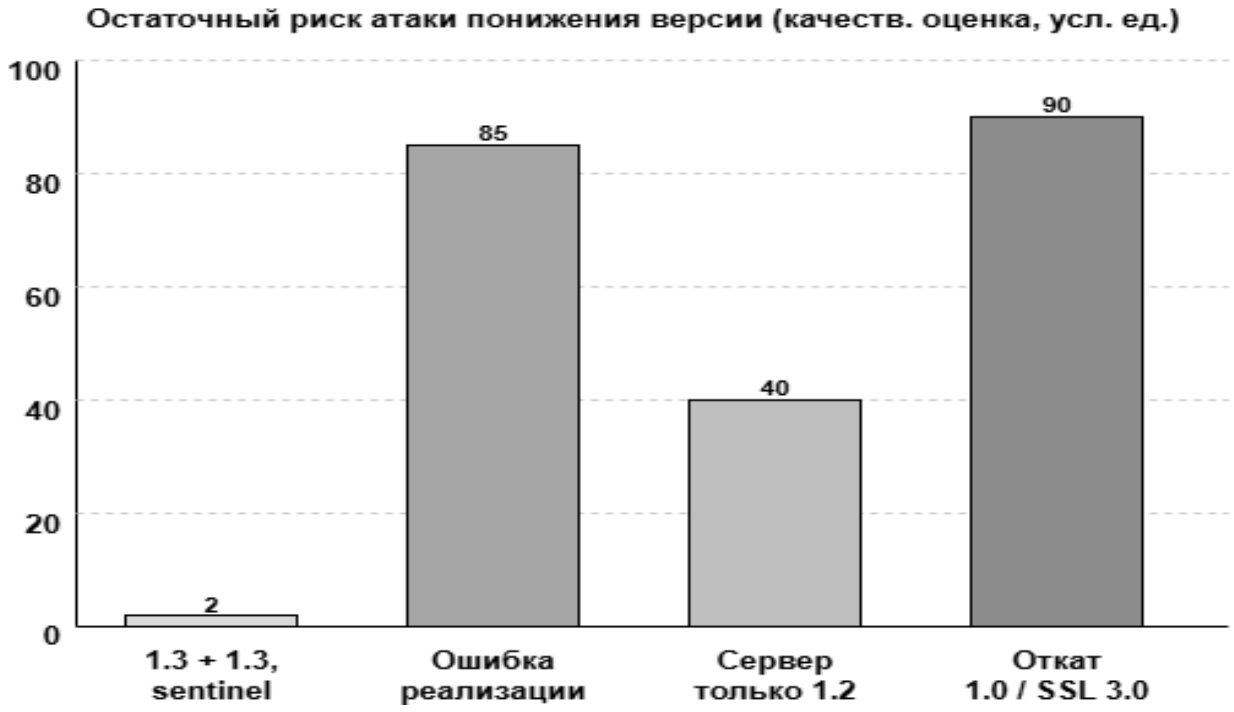

Рисунок 2. Остаточный риск атаки понижения версии по сценариям

Рекомендации.

По результатам проведённого анализа для практической защиты от атак понижения версии целесообразно: отключать на клиенте и сервере поддержку версий ниже TLS 1.2, а по возможности – использовать только TLS 1.3; обеспечивать обязательную проверку контрольного значения downgrade sentinel на стороне клиента и подтверждать её наличие при аудите реализаций; применять сигнальный набор TLS_FALLBACK_SCSV для сценариев с откатом; проводить мониторинг согласуемых версий и выявлять аномальные понижения; отключать режим ранних данных 0-RTT для чувствительных операций. Эшелонирование указанных мер, как следует из выражения (3), обеспечивает устойчивость защиты к отказу отдельных механизмов.

Заключение.

В работе рассмотрены уязвимости протокола TLS 1.3, связанные с атаками понижения версии, и оценена эффективность встроенных мер противодействия. Установлено, что механизм downgrade sentinel в сочетании с проверкой подписи и завершающим сообщением Finished обеспечивает надёжное обнаружение активного понижения версии при условии, что обе стороны поддерживают TLS 1.3 и корректно реализуют проверку. Предложенная модель остаточного риска показывает, что итоговая защищённость определяется прежде всего корректностью реализации и настройкой допустимых версий на оконечных узлах, а также эшелонированием защитных механизмов. Полученные результаты могут быть использованы при аудите и настройке подсистем защищённого обмена данными в телекоммуникационных системах.

Список литературы:

1. Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. – IETF, 2018. – 160 p.

2. Dierks T., Rescorla E. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246. – IETF, 2008. – 104 p.

3. Moeller B., Langley A. TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks. RFC 7507. – IETF, 2015. – 8 p.

4. Moeller B., Duong T., Kotowicz K. This POODLE Bites: Exploiting the SSL 3.0 Fallback. – Google, 2014. – 4 p.

5. Adrian D. et al. Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice // Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS). – 2015. – P. 5-17.

6. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на С. – М.: Диалектика, 2018. – 1040 с.

7. Шевчук П. С. Криптографическая защита информации: учебник. – Москва: РИОР: ИНФРА-М, 2018. – 321 с.