ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 29 МАТЕМАТИКИ Выпуск 3
2022

А. А. Елистратов, **Н. В. Никонов**, **Н. А. Полховский**, **Е. Д. Шупляк** (Москва, Деп. информ. безопасности Банка России, ТК 26, Лаб. ТВП, ФУМО ВО ИБ)**. Об особенностях реализации протоколов семейства (D)TLS с позиции скорости соединения и возможности проведения паддинг-атак.**

УДК 004.057.4 DOI https://doi.org/10.52513/08698325_2022_29_3_1

Резюме: предложен способ повышения скорости (D)TLS-взаимодействия за счет передачи сообщений (D)TLS в рамках одной UDP-датаграммы (для DTLS) или TCP-сегмента (для TLS). Однако обращено внимание на то, что такой способ может привести к повышению эффективности проведения паддинг-атак на DTLS.

Ключевые слова: паддинг-атака, ТК26, TLS, DTLS.

Протоколы TLS (Transport Layer Security) нашли свое широкое применение при обеспечении защищенного доступа к веб-ресурсам, соответствующие протоколы DTLS (Datagram TLS) все чаще используются при построении VPN-сетей (Virtual Private Network). Протоколы семейства (D)TLS поддерживают использование блочной шифрсистемы в режиме шифрования CBC, требующего дополнения последнего неполного блока открытых данных до полного байтами структурированного вида — *паддингом* (от англ. padding). При этом контроль целостности сообщений за счет добавления кода аутентичности производится до шифрования данных. Известно, что такие варианты TLS могут быть подвержены паддинг-атакам [1, 2]. Общую идею паддинг-атак [3] можно распространить и на случай использования режимов шифрования, отличных от CBC [4], когда роль паддинга будут играть некоторые фиксированные поля, например, внутренних или специальных сообщений TLS [5].

Все это повлияло на появление новой версии протокола TLS 1.3 (RFC 8446), которая использует только *аутентифицированное шифрование* и лишено недостатков предыдущих версий протоколов. Данная инициатива была поддержана и российской стороной и в рамках работы «Криптографическая защита информации» Технического комитета по стандартизации ТК26 были разработаны рекомендации [6], получены идентификаторы IANA на соответствующие российские криптонаборы. В рамках ТК26 была проведена работа по подготовке контрольных примеров по реализации российского варианта TLS 1.3 для предотвращения потенциальных проблем с совместимостью.

Было установлено, что отечественная реализация оказалась в среднем в полтора раза медленнее, чем реализация протокола TLS 1.3 на основе криптобиблиотеки OpenSSL со схожим криптонабором AES_GCM_256_SHA256, что может быть обусловлено аппаратной поддержкой алгоритма шифрования AES.

Был предложен способ объединения пакетов, отправляемых сторонами, в рамках одного TCP-сегмента. Реализация этой идеи приблизила среднее время установления соединения к зарубежным аналогам. Однако, авторы указывают на то, что реализация этой идеи применительно для протоколов DTLS может привести к возникновению более эффективных, чем для TLS, паддинг-атак.

В исходной идее паддинг-атаки [3] из зашифрованных блоков

$$y_1, y_2, \ldots, y_n, \quad y_i = ENC(x_i \oplus y_{i-1}), \qquad i = 1, 2, \ldots, n$$

(где y_0 — вектор инициализации IV, x_i — блоки открытых данных), формируются сообщения вида

$$Y = \ldots y_{i-1} \oplus r, y_i$$

(r — случайный блок), которые передаются на веб-ресурс для расшифрования. Установление факта корректности паддинга у последнего расшифрованного блока

$$ENC^{-1}(y_i) \oplus y_{i-1} \oplus r = x_i = x_i \oplus r$$

позволяет найти байты блока

$$x_i : x_i = \ldots PAD \oplus r.$$

Различение гипотез о корректности и некорректности обычно достигается статистическими методами и требует проведения большого числа экспериментов по передаче сообщений вида Y с учетом того, что MAC будет всегда неверным и это повлечет разрыв соединения.

В соответствии с RFC 6347 в протоколе DTLS пакеты с неверным VFC рекомендовано игнорировать, при этом соединение будет продолжено, и нет подобных указаний для сообщений с некорректным PAD. Но учитывая, что для защиты от паддинг-атак ошибки при MAC/PAD-проверке должны быть неразличимы, разумно предположить, что соединение будет продолжено и при некорректном PAD.

Предположим, что на сервер в одной DTLS сессии одновременно передается большое количество DTLS-сообщений вида Y (с корректными заголовками HDR^i_{DTLS}, $i = 1, 2, \ldots, n$):

$$HDR_{UDP} \| HDR^1_{DTLS}, Y \| \ldots \| HDR^n_{DTLS}, Y \| HDR^{n+1}_{DTLS}, Z, \qquad (1)$$

а обработка сообщения Z приводит к произвольному ответу сервера (например, содержит некорректный заголовок DTLS-пакета HDR^{n+1}_{DTLS}).

Сообщения могут быть переданы как в одной UDP-датаграмме вида (1), так и в нескольких таких UDP-датаграммах. Получив такую UDP-датаграмму, сервер начнет обработку содержащихся в нем DTLS сообщений последовательно и будет игнорировать сообщения, не прошедшие MAC/PAD-проверку. Таким образом, сервер последовательно обработает все принятые DTLS сообщения, затем перейдет к обработке сообщения Z, при обработке которого в канале связи появится ответ.

Изложенное выше дает авторам основание обратить внимание на то обстоятельство, что совокупность описанных выше свойств DTLS может быть использована для повышения эффективности паддинг-атак, использующих временные характеристики для различения статистических гипотез за счет увеличения средней разницы времени ответа сервера на сообщения с корректным/некорректным PAD в n раз, и это необходимо учитывать синтезе протоколов DTLS.

СПИСОК ЛИТЕРАТУРЫ

1. Scalable Scanning and Automatic Classification of TLS Padding Oracle Vulnerabilities. USENIX Security, 2019. *Merget R.*, *Somorovsky J.*, *Aviram N.*, *Young C.*, *Fliegenschmidt J.*, *Schwenk J.*, *Shavitt Y.* Scalable scanning and automatic classification of TLS padding oracle vulnerabilities. In: Proceedings of the 28th USENIX Security Symposium. (Santa Clara, CA, August 14–16, 2019.) Berkeley, CA: USENIX Ass., 2019, p. 1029–1046.

2. *Бирюков Д. С.*, *Елистратов А. А.*, *Ларионов В. В.*, *Никонов Н. В.*, *Самойлов А. А.* О возможных модификациях временных паддинг-атак на протоколы семейства TLS. — Обозрение прикл. и промышл. матем., 2017, т. 24, в. 5. // *Biryukov D. S.*, *Elistratov A. A.*, *Larionov V. V.*, *Nikonov N. V.*, *Samoilov A. A.* On possible modifications of timing padding attacks on TLS family of protocols. — OP&PM Surv. Appl. Industr. Math., 2017, т. 24, в. 5. (In Russian.)

3. *Vaudenay S.* Security flaws induced by CBC padding — applications to SSL, IPSEC, WTLS. . . . In: Advances in Cryptology–EUROCRYPT 2002. International Conference on the Theory and Applications of Cryptographic Techniques. (Amsterdam, April 28–May 2, 2002.) Proceedings. / Ed. by L. R. Knudsen. Heidelberg etc.: Springer, 2002, p. 534–545. (Ser. Lect. Notes Comput. Sci. V. 2332.)

4. *Елистратов А. А.*, *Никонов Н. В.*, *Шумилов А. О.* О паддинг-атаках на криптографические протоколы, использующие стандартные n-разрядные блочные режимы шифрования. — Обозрение прикл. и промышл. матем., 2014, т. 21, в. 4, с. 358–360. // *Elistratov A. A.*, *Nikonov N. V.*, *Shumilov A. O.* Padding attacks on cryptographic protocols using standard n-tuples block encryption schemes. — OP&PM Surv. Appl. Industr. Math., 2014, v. 21, is. 4, p. 358–360. (In Russian.)

5. *Елистратов А. А.*, *Никонов Н. В.*, *Ларионов В. В.*, *Свистюр З. В.* О возможности использования внутренних сообщений протокола TLS для проведения паддинг-атак. — Обозрение прикл. и промышл. матем., 2020, т. 27, в. 2, с. 143–145. // *Elistratov A. A.*, *Nikonov N. V.*, *Larionov V. V.*, *Svistyur Z. V.* On the possibility of using internal protocol messages TLS for padding attacks. — OP&PM Surv. Appl. Industr. Math., 2020, т. 27, в. 2, с. 143–145. (In Russian.)

6. Р 1323565.1.030-2020. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3). М.: Стандартинформ, 2020. // Р 1323565.1.030-2020. The Use of the Russian Cryptographic Algorithms in the Transport Layer Security Protocol (TLS 1.3) Information technology. Cryptographic Data Security. Moscow.: StandardInform, 2020.

Поступила в редакцию
26.IX.2022

UDC 004.057.4 DOI https://doi.org/10.52513/08698325_2022_29_3_1

Elistratov A. F., ***Nikonov N. V.***, ***Polchovskii N. A.***, ***Shuplyak E. D.*** (Moscow, Information Security Department of the Bank of Russia, Technical Committee 26, TVP Laboratories, FUMO VO IS Federal Educational and Methodological Association for Higher Education in Information Security **. About the increasing of (D)TLS-communication's speed and possibility of padding oracle attacks.**

Abstract: A method to make DTLS-connections more effective is suggested. The method is based on aggregation of DTLS fragments into one UDP-datagram (for DTLS) or TCP-segment (for TLS). On the contrary, it may increase the effectiveness of padding oracle attacks on DTLS.

Keywords: DTLS, padding oracle attack, TC26, VPN.