УДК 004.056.55
DOI: 10.17586/0021-3454-2018-61-1-60-64

МОДИФИКАЦИЯ ПРОТОКОЛА TLS НА ОСНОВЕ РАЗРЕЖЕННОЙ КРИПТОСИСТЕМЫ С ОБЩЕЙ ПАМЯТЬЮ

А. Д. Метлинов

Владимирский государственный университет им. А. Г. и Н. Г. Столетовых, 600000, Владимир, Россия
E-mail: lexlotr@gmail.com

Рассматриваются особенности модификации протокола TLS с помощью модели рюкзачной криптосистемы с общей памятью. Существующие на сегодняшний день протоколы безопасности передачи сообщений по каналам связи имеют значимые недостатки и не являются абсолютно безопасными для передачи информации. Для повышения эффективности организации защищенного канала связи в сетях TCP/IP предложено в дополнение к существующим криптоалгоритмам использовать на всех этапах работы протокола TLS алгоритмы симметричной рюкзачной криптографии, CBC-блочного варианта симметричной рюкзачной криптосистемы и хеш-функции на его основе.

Ключевые слова: *общая память, протокол TLS, криптографические рюкзаки, блочный шифр с режимом зацепления блоков, сети TCP/IP, канал связи, модификации протокола*

Модель криптографической симметричной системы с общей памятью, основанная на задаче об укладке рюкзака, была представлена в работе [1]. Аналогичная модель, построенная на возвратных базисах, без использования общей памяти и в более общей постановке рассматривается в работе американских специалистов [2—4]. Некоторые обобщения этой схемы при использовании возвратных (линейно-рекуррентных) последовательностей порядка $m \geq 2$ в качестве базиса укладки рюкзака приведены в работе [5], где также описаны статистические свойства криптосистемы для случая $m = 2$. Кроме того, в этой же работе показана возможность объединения представленной алгоритмической схемы с другими стандартами шифрования или ее применения в протоколах передачи данных (например, https). Использование этой алгоритмической схемы для модификации протокола TLS подробно обсуждается в настоящей статье.

Основа телекоммуникационной сети — стек протоколов TCP/IP, поэтому часто такая сеть носит название „сеть TCP/IP“ и представляет собой множество каналов связи (КС) между отправителями и получателями. Рассмотрим особенности каналов связи в сетях TCP/IP, принципиальные для обеспечения безопасности передачи сообщений от узла (отправителя — Sender) к серверу (получателю — Receiver):

— КС не имеет встроенных средств защиты передаваемых сообщений;

— основные механизмы обеспечения информационной безопасности (ИБ) КС реализованы на сеансовом уровне сетевой модели OSI и имеют множество уязвимостей;

— основные угрозы и атаки в КС направлены на перехват передаваемых сообщений — угрозы конфиденциальности и целостности данных; незначительное количество атак относится к атакам на доступность узлов канала и их подмену;

— приоритетным направлением обеспечения ИБ КС является использование криптографических механизмов защиты;

— при обеспечении ИБ КС предполагается, что злоумышленник во внешней среде присутствует всегда и обладает неограниченными вычислительными ресурсами [6].

Основные направления повышения эффективности использования протоколов защиты информации в КС сетей TCP/IP — увеличение скорости работы (быстродействия алгоритмов, лежащих в их основе) и повышение криптостойкости. Предлагаемые подходы рассмотрим на примере протокола TLS.

Протокол TLS (Transport Layer Security) используется для обеспечения конфиденциальности и целостности данных при объединении двух приложений. В результате соединение является конфиденциальным, если для шифрования данных используется симметричная криптография, ключи генерируются независимо для каждого соединения с использованием секретного кода, получаемого с помощью другого протокола; соединение является надежным, если процедура передачи сообщения включает в себя проверку целостности с помощью вычисления кода аутентификации MAC, для расчета которого используются хэш-функции.

Общий граф работы протокола TLS с потенциально уязвимыми местами *1—3* представлен на рис. 1.

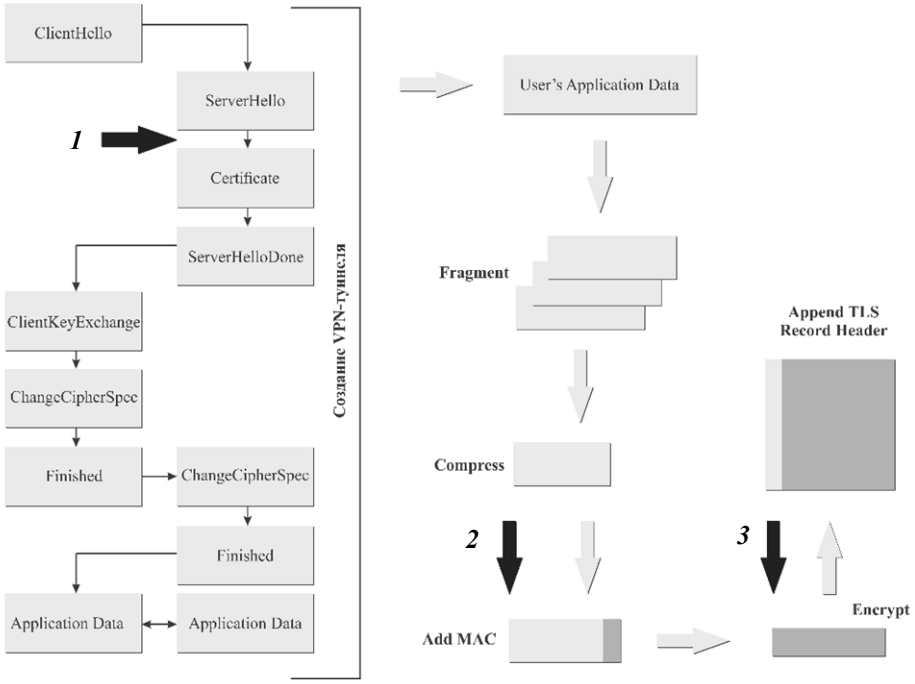

Рис. 1

Уязвимость 1. Вследствие многообразия используемых алгоритмов асимметричной криптографии с разными длинами ключей возможно осуществление MITM-атаки (рис. 2). Таким образом, все последующие передаваемые данные будут дискредитированы и известны злоумышленнику.

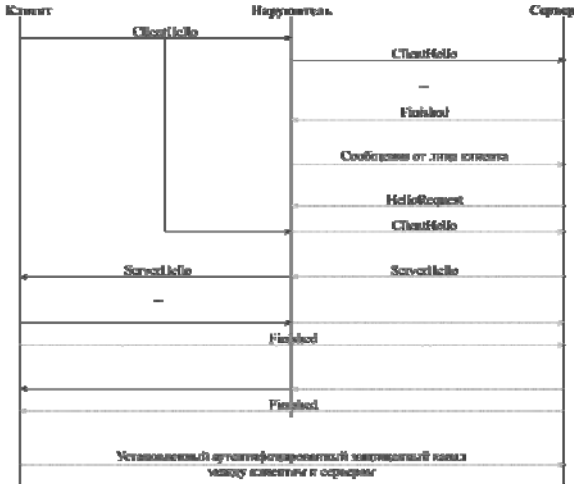

Рис. 2

Для генерации сеансовых ключей (при аутентификации сервера и клиента) на этапе создания VPN-туннеля вместо медленного алгоритма RSA (или других асимметричных алгоритмов) представляется возможным следующие:

— использование асимметричного варианта рюкзачной криптосистемы с *pre-shared key* в виде общей памяти;

— использование для генерации *Master Secret* уникальной для пары клиент—сервер хеш-функции на основе данной симметричной рюкзачной криптосистемы.

Уязвимость 2. В протоколе TLS код MAC в той или иной форме содержится во всех зашифрованных записях. Способ вычисления кода аутентификации зависит от применяемого набора шифров и режима шифрования. Код HMAC — MAC, основанный на криптографической хеш-функции, используется, например, с шифрами протокола TLS в режиме CBC. HMAC вычисляется независимо от функции шифрования. Более того, MAC изначально используется неверно: сперва для открытого текста вычисляется HMAC, а потом сообщение с присоединенным кодом аутентификации шифруется. Именно так работает режим CBC в TLS. Внутри записи защищенные данные размещаются вместе с кодом аутентификации, и то, и другое зашифровано. Проблема заключается в том, что MAC можно проверить только после расшифровки сообщения, и, если значение оказалось некорректным, при выполнении TLS должно появиться сообщение об ошибке. В этом случае активный злоумышленник, изменяя шифрованный текст, может использовать расшифровывающий узел в качестве криптографического „оракула“, который постепенно раскроет весь секретный текст. На этом основано несколько практических атак на протокол TLS.

Для обхода этой проблемы на основе реализации рюкзачного симметричного блочного шифра с помощью стандартной схемы свертки блоков за счет общей памяти можно построить стандартный алгоритм хеширования, применяемый для контроля достоверности передаваемой информации от отправителя к получателю. Свертка блочного шифра порождает такую хэш-функцию для пары Sender—Receiver, которая является строго индивидуальной и свободна от вышеописанных недостатков.

Уязвимость 3. В дополнение к применяемым в основе набора шифров протокола TLS стандартным алгоритмам (RC2, RC4, AES, DES, 3DES и т.п.) предлагается использовать алгоритмы преобразования информации с помощью CRC-блочного варианта симметричной рюкзачной криптосистемы с общей памятью, которая, по сути, является аналогом *pre-shared key*.

Пусть под скоростью работы протокола TLS понимается величина

$$\mathrm{IPS}(\mathrm{TLS}) = \frac{1}{T_{\text{auth}} + T_{\text{frag}} + T_{\text{cmps}} + T_{\text{MAC}} + T_{\text{enc}}},$$

где T_{auth} — время работы алгоритма аутентификации клиента и сервера; T_{frag} — время работы алгоритма фрагментации сообщений; T_{cmps} — время работы алгоритма компрессии сообщений; T_{MAC} — время работы алгоритма создания кода аутентификации сообщений; T_{enc} — время работы симметричных блочных алгоритмов шифрования и дешифрования сообщений.

Согласно результатам скоростных тестов [5] можно предположить, что разрабатываемые алгоритмы выигрывают по быстродействию (симметричные рюкзачные шифры одни из самых быстрых на данный момент) и криптостойкости, так как обладают криптостойкостью к атакам, которым подвержены шифры из стандартных наборов; эти алгоритмы построены для работы в различных режимах.

Использование предложенной криптосистемы на таких этапах работы протокола TLS, как аутентификация клиента и сервера, создание кода аутентификации сообщений и работа симметричных блочных алгоритмов шифрования и дешифрования сообщений, позволяет

существенно уменьшить величины T_{auth}, T_{MAC} и T_{enc}, что в соответствии с вышеприведенной формулой способствует увеличению значения $\text{IPS}(\text{TLS})$, т.е. повышению быстродействия и эффективности протокола TLS.

По сравнению с существующими версиями рюкзачных криптографических систем новыми являются следующие положения:

— введение общей памяти (*shared memory*) для пары Sender—Receiver, недоступной злоумышленнику в КС;

— отказ от супервозрастающих базисов в пользу возвратных последовательностей порядка m, где $m \geq 2$ [5].

На основании вышеизложенного можно сделать вывод, что все существующие на сегодняшний день протоколы безопасности передачи сообщений в КС имеют собственные значимые недостатки и не являются абсолютно безопасными для передачи информации в КС сетей TCP/IP.

Для повышения эффективности организации защищенного канала связи в сетях TCP/IP с помощью TLS предложено использовать разработанные алгоритмы асимметричной рюкзачной криптографии, CBC-блочного варианта симметричной рюкзачной криптосистемы и хеш-функции на его основе.

Спроектированное семейство CBC-блочных алгоритмов криптосистемы с общей памятью, независимо от типа и объема исходных данных, работает в среднем на 7—9 % быстрее, чем функция DH_AES в стандартном наборе шифров протокола TLS, и на 25—28 % быстрее, чем рюкзачная криптосистема, в основе которой лежит супервозрастающий базис. Использование предложенных алгоритмов значительно повышает скорость работы [7, 8] данного протокола в канале связи за счет быстрого блочного рюкзачного шифрования, уменьшает время создания сессии между сервером и клиентом при двусторонней аутентификации, а также повышает криптостойкость системы благодаря общей памяти, недоступной противнику в модели Долев — Яо, как в режиме чтения, так и в режиме подмены.

СПИСОК ЛИТЕРАТУРЫ

1. *Александров А. В., Метлинов А. Д.* Симметричная рюкзачная криптосистема с общей памятью и плотностью укладки больше единицы // Изв. вузов. Приборостроение. 2015. Т. 58, № 5. С. 344—350.

2. *Hamlin N., Krishnamoorthy B., Webb W.* A knapsack-like code using recurrence sequence representations // Fibonacci Quarterly. 2015. N 1 (53). P. 24—33,

3. *Merkle D. R., Hellman M.* Hiding information and signatures in trapdoor knapsacks // Information Theory, IEEE Transact. 1978. P. 525—530.

4. *Odlyzko A. M., Lagarias J. C.* Solving low-density subset sum problems // J. Association Computing Machinery. 1985. Vol. 32, N 1. P. 229—246.

5. *Александров А. В., Метлинов А. Д.* Алгоритмические и статистические свойства разреженной рюкзачной криптосистемы с общей памятью // Изв. вузов. Приборостроение. 2017. Т. 60, № 1. С. 5—9.

6. *Dolev D., Yao A.* On the security of public key protocols // IEEE Transact. on Inform. Theory. 1983. Vol. 29, N 2. P. 198—208.

7. *Метлинов А. Д.* Скоростные характеристики симметричной рюкзачной криптосистемы с общей памятью и плотностью укладки больше единицы. NIST - тестирование // Сб. науч. тр. III Междунар. науч.-практ. конф. „Информационная безопасность в свете Стратегии Казахстан — 2050“. 2015. С. 247—252.

8. *Метлинов А. Д.* О скоростных особенностях и NIST-тестировании симметричной рюкзачной криптографической системы с общей памятью // Сб. тр. XI Междунар. науч. конф. „Перспективные технологии в средствах передачи информации“. 2015.

Сведения об авторе

Александр Дмитриевич Метлинов — аспирант; ВлГУ, кафедра информатики и защиты информации; E-mail: lexlotr@gmail.com

Поступила в редакцию
15.09.17 г.

Ссылка для цитирования: *Метлинов А. Д.* Модификация протокола TLS на основе разреженной криптосистемы с общей памятью // Изв. вузов. Приборостроение. 2018. Т. 61, № 1. С. 60—64.

MODIFICATION OF THE TLS PROTOCOL ON THE BASIS OF A LOW-DENSITY CRYPTOSYSTEM WITH SHARED MEMORY

A. D. Metlinov

Vladimir State University, 600000, Vladimir, Russia
E-mail: lexlotr@gmail.com

Features of the TLS protocol modifications with the use of a model of knapsack cryptosystem with shared memory are considered. The existing security protocols for the transmission of messages in the communication channel are shown to have their own significant disadvantages and therefore to be not quite safe for information transmission. To improve the efficiency of the organization of a secure communication channel in TCP/IP networks, it is proposed to use algorithms of symmetric backpack cryptography, a CRC-variant of a symmetric backpack cryptosystem, and a hash function based on it additional of the existing crypt algorithms at all stages of the TLS protocol operation.

Keywords: shared memory, TLS protocol, cryptographic knapsacks, a block cipher with a block mode of engagement, TCP/IP networks, communication channel, protocol modifications

Data on author

Aleksander D. Metlinov — Post-Graduate Student; Vladimir State University, Department of Information and Information Security; E-mail: lexlotr@gmail.com

For citation: Metlinov A. D. Modification of the TLS protocol on the basis of a low-density cryptosystem with shared memory. *Journal of Instrument Engineering*. 2018. Vol. 61, N 1. P. 60—64 (in Russian).

DOI: 10.17586/0021-3454-2018-61-1-60-64