ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 24 МАТЕМАТИКИ Выпуск 5
2017

А. Е. Архипов, **Р. А. Кравцов**, **В. В. Мкртичян** (Ростов-на-Дону, ЮФУ ММиКН)**. Оптимизированный протокол генерации сеансового ключа с защитой от атак типа «человек-посередине» при использовании асимметричных ключей одним пользователем протокола.**

В [1] Б. Шнайер рассматривает протоколы генерации сеансового ключа, а в [2] А. Черемушкин анализирует их, в частности, показывает, что TLS защищен от атак типа «человек–посередине» посредством связки протоколов [2, с. 122] DH (Диффи–Хеллман) [1, с. 378] и RSA [1, с. 346]. Построим криптографический протокол путем улучшения этой связки. Пусть Алиса(α) и Боб(β) — участники протокола, являющиеся клиентом и сервером соответственно, S и S' — симметричные шифросистемы, которые могут совпадать, A — асимметричная шифросистема, k_o и k_c — открытый и закрытый ключи соответственно шифросистемы A [1, с. 35–38], $E_k^C(M)$ — функция зашифрования сообщения M на ключе k в шифросистеме C, $D_k^C(M)$ — функция расшифрования сообщения M на ключе k в шифросистеме C.

Целью протокола является выработка сеансового ключа t для шифросистемы S.

Входные данные. Со стороны Алисы требуется т.н. «мастер-ключ» k шифросистемы S. Со стороны Боба требуется наличие k_o и k_c шифросистемы A, выданные удостоверяющим центром.

Выходные данные. Выходными данными для обоих сторон будет сгенерированный сеансовый ключ t шифросистемы S. Шифросистемы S и S' могут совпадать.

Шаг 1. Алиса проверяет валидность k_o и, если проверка прошла успешно, генерирует «мастер-ключ» k, после чего отправляет Бобу следующее сообщение:

$$\alpha \to \beta: \ E_{k_o}^A(k).$$

Шаг 2. С помощью k_c Боб расшифровывает полученное сообщение и получает k:

$$\beta: \ D_{k_c}^A(E_{k_o}^A(k)) = k.$$

Шаг 3. Алиса и Боб вместе выбирают большие простые числа g и n так, чтобы g являлось примитивным корнем по модулю n и обмениваются ими по незащищенному каналу.

Шаг 4. Боб выбирает случайное большое целое число x и отправляет Алисе следующее сообщение:

$$\beta \to \alpha: \ E_k^S(X), \text{ где } X = g^x \mod n.$$

Шаг 5. Алиса выбирает случайное большое целое число y и отправляет Бобу следующее сообщение:

$$\alpha \to \beta: \ E_k^S(Y), \text{ где } Y = g^y \mod n.$$

Шаг 6. Боб вычисляет следующие значения:

$$\beta: \ D_k^S(E_k^S(Y)) = Y, \ t = Y^x \mod n.$$

Шаг 7. Алиса вычисляет следующие значения:

$$\alpha: \ D_k^S(E_k^S(X)) = X, \ t' = X^y \mod n.$$

Заметим, что $t = t'$, действительно:

$$t = Y^x \mod n = g^{yx} \mod n = g^{xy} \mod n = X^y \mod n = t'.$$

Далее, Алиса и Боб могут обмениваться зашифрованными данными по открытому каналу связи посредством шифосистемы S используя ключ t.

Лемма. *Данный протокол защищен от угроз типа «человек–посередине». Основным его преимуществом перед связкой DH и RSA, которая также защищена от угроз типа «человек–посередине», является меньшее количество операций асимметричного шифрования, что делает процесс его выполнения менее ресурсоемким.*

Доказательство. В отличие от протокола DH, представленный выше протокол защищен от угрозы типа «человек–посередине». Защита обеспечивается зашифрованием промежуточных вычислений на шагах (4)–(7) с помощью шифросистемы S на ключе k. Благодаря этому у злоумышленника пропадает возможность их подмены в процессе выполнения протокола, а значит и осуществить атаку типа «человек-посередине» Оптимизация достигается «вынесением» операций асимметричного шифрования из шагов (4)–(7) в шаги (1)–(2) протокола, что уменьшает количество асимметричных операций в два раза относительно протокола связки DH и RSA, в которой подписывается каждая часть протокола DH. □

Замечание. Такая оптимизация наиболее важна для малопроизводительных устройств.

СПИСОК ЛИТЕРАТУРЫ

1. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002, 610 с.
2. *Черемушкин А. В.* Криптографические протоколы. Основные свойства и уязвимости: учебное пособие. М.: Академия, 2009, 272 с.
3. The Transport Layer Security (TLS) Protocol Version 1.2 [Electronic resource]. — URL: https://tools.ietf.org/html/rfc5246 (дата обращения 11.06.2017)