СТАНДАРТИЗАЦИЯ АЛГОРИТМОВ РАЗДЕЛЕНИЯ СЕКРЕТА В РЕСПУБЛИКЕ БЕЛАРУСЬ

УДК 004.056.53 (003.26)

Н.Н. Шенец,
НИИ ППМИ БГУ, г. Минск

Аннотация

Рассматриваются алгоритмы разделения секрета. Указываются изменения, внесенные в проект стандарта Республики Беларусь СТБ 34.101.60 «Информационные технологии и безопасность. Алгоритмы разделения секрета».

Введение

Теория разделения секрета зародилась в работах А. Шамира [1] и Г. Блейкли [2] в связи с решением следующей задачи. Пусть имеется некоторая важная информация (секрет) S, доступ к которой нельзя доверить одному лицу, а требуется так распределить ее в виде частичных секретов между пользователями, чтобы лишь заранее определенные подмножества этих пользователей (разрешенные подмножества), объединяя свои частичные секреты, могли восстановить исходный секрет. Остальные подмножества пользователей называются запрещенными и не могут восстановить секрет. Алгоритмы, решающие данную задачу, называются схемами разделения секрета.

В настоящее время данная теория нашла много применений: протоколы электронного голосования, пороговая криптография (пороговые схемы электронной цифровой подписи), помехоустойчивое кодирование, широковещательное шифрование и распределенные секретные вычисления. Были разработаны критерии качества схем разделения секрета [3], наиболее важными из которых являются совершенность и идеальность. Совершенность означает, что запрещенные подмножества пользователей, объединив свои частичные секреты, не получают никакой информации об исходном значении секрета, кроме априорной. Идеальными называются совершенные схемы разделения секрета, в которых размеры частичных секретов совпадают с размером секрета.

В НИИ ППМИ был разработан предварительный стандарт Республики Беларусь СТБ П 34.101.60 2011 «Информационные технологии и безопасность. Алгоритмы разделения секрета» [4], действие которого прекращается летом текущего года. В этой связи в нашей организации ведутся работы по переводу данного предварительного стандарта в стандарт Республики Беларусь. При этом в проект стандарта внесены существенные изменения и дополнения. Данные изменения учитывают то обстоятельство, что некоторые компании уже реализовали алгоритмы из предварительного стандарта и даже провели их экспертизу.

Основная часть

Предварительный стандарт СТБ П 34.101.60 2011 основывается на идеальной модулярной схеме разделения секрета в кольце многочленов от одной переменной над двоичным полем [5–6]. Эта схема разделения секрета состоит из алгоритмов генерации параметров, алгоритма разделения секрета и алгоритма восстановления секрета. Она является пороговой, т.е. среди n пользователей разрешенными подмножествами являются любые подмножества, состоящие из t или более пользователей. Число t называется пороговым числом.

Параметрами схемы разделения секрета являются: общее число пользователей n, пороговое число t, длина секрета l в битах, общий открытый ключ M_0 и открытые ключи пользователей $M_1, \ldots, M_n$ длиной l битов каждый. Открытые ключи необходимо генерировать либо задавать из таблиц.

В СТБ П 34.101.60 2011 определено два алгоритма генерации открытых ключей, а также приведены таблицы возможных ключей для $l \in \{128, 192, 256\}$. Оказалось, что предложенные в предварительном стандарте алгоритмы не являются, на сегодняшний день, оптимальными. В проекте стандарта данные алгоритмы заменены новыми, которые имеют лучшую вычислительную скорость. Более того, генерация общего открытого ключа вынесена в отдельный алгоритм, добавлен алгоритм генерации открытого ключа пользователя по идентификатору пользователя, что, несомненно, будет востребовано на практике.

Изменения коснулись также и параметра l. Если в СТБ П 34.101.60 2011 допускалось выбирать произвольное число l, кратное 8, то в проекте стандарта зафиксировано 3 значения $l \in \{128, 192, 256\}$. Это связано, в первую очередь, с тем, что в современной криптографии данные длины наиболее часто используются. Кроме того, скорость алгоритмов разделения и восстановления секрета напрямую зависит от параметра l и с его увеличением заметно возрастает. Фиксация параметра l упрощает программную реализацию алгоритмов стандарта.

Алгоритмы разделения и восстановления секрета остались в неизменном виде, что, безусловно, важно разработчикам, уже реализовавшим данные алгоритмы. Однако в проект стандарта в качестве приложений добавлено два новых режима использования схемы разделения секрета.

Первый из них касается свойства проверяемости секрета после его восстановления. Если частичные секреты некорректные, то восстановленное значение также не будет совпадать с истинным значением секрета. Поэтому с целью обнаружения такого события в проекте стандарта предлагается использовать функцию хэширования. При этом на частичные секреты разделяется пара $(S, h, (S))$, и каждый пользователь i получает пару значений S_i, H_i. После восстановления секрета пользователи проверяют, что вторая половинка восстановленного значения является хэшем от первой. Если это не так, то какие-то частичные секреты пользователей некорректны, а восстановленное значение не является секретом.

Второй режим связан с тем обстоятельством, что в реальных системах может не быть стороны (дилера), которая знает секрет и самостоятельно его разделяет, а затем распределяет частичные секреты. В этой ситуации необходим протокол одновременной выработки секрета пользователями и разделения его на частичные секреты. Такой протокол существует, и он предложен в одном из приложений проекта стандарта.

Заключение

Таким образом, в НИИ ППМИ разработан стандарт по разделению секрета, востребованный в Республике Беларусь. Отметим, что в настоящее время ни в одной стране мира пока не принят аналогичный стандарт. Единственным известным нам аналогом является интернет-драфт [7], который действовал в 2009 году в течение полугода. Он основан на схеме Шамира и в вычислительном аспекте лучше нашего стандарта, однако при этом общее число пользователей в системе не должно быть больше 255, за счет чего и достигается выигрыш в скорости.

Литература:

1. Shamir, A. How to share a secret. – Comm. ACM, 1979. – V. 22. – P. 612–613.

2. Blakley, G. Safeguarding cryptographic keys. – Proc. AFIPS Nat. Comp. Conf., 1979. – V. 48. – P. 313–317.

3. Stinson D. R. Cryptography: Theory and Practice. – CRC Press, 2002.

4. СТБ П 34.101.60–2011 «Информационные технологии и безопасность. Алгоритмы разделения секрета», Госстандарт 2011, URL: http://tnpa.by/KartochkaDoc.php?UrlRN=261838&UrlIDGLOBAL=359544.

5. Galibus, T. Some structural and security properties of the modular secret sharing / T. Galibus, G. Matveev, N. Shenets. – SYNASC'2008 IEEE Comp. Soc., CPS, Los Alamitos, 2009. – P. 197–200.

6. Шенец, Н.Н. Об информационном уровне модулярных схем разделения секрета / Н.Н. Шенец // Докл. Нац. акад. наук Беларуси, сер. физ.-мат. наук, 2010. – Т. 54, № 6. – С. 9–12.

7. Threshold Secret Sharing: draft-mcgrew-tss-02, URL: http://tools.ietf.org/html/draft-mcgrew-tss-02.

Abstract

The secret sharing algorithms are considered. Modifications of the Belarusian standard STB 34.101,60-2011 «Information technology and security. Secret sharing algorithms» are specified.

Поступила в редакцию 18.05.2013 г.

СТАНДАРТИЗАЦИЯ ПРОТОКОЛА TLS В РЕСПУБЛИКЕ БЕЛАРУСЬ

УДК 004.056.55 (003.26)

С.В. Агиевич, О.В. Соловей,
НИИ ППМИ БГУ, г. Минск

Аннотация

Протокол TLS стандартизируется в Республике Беларусь. В разрабатываемый стандарт будут включены дополнительные криптонаборы TLS, основанные на отечественных криптографических алгоритмах. В работе описываются дополнительные криптонаборы, а также связанные с ними методы аутентификации.

Введение

Для защиты соединений между клиентом и сервером в сети Интернет в большинстве случаев применяется протокол TLS (Transport Layer Security). TLS обеспечивает взаимную аутентификацию сторон протокола, конфиденциальность и контроль целостности передаваемых между сторонами данных. Последняя на сегодняшний день редакция TLS определена в RFC 5246 [1]. Стандартизация этой редакции завершается сейчас в Республике Беларусь. Предполагается, что в текущем году будет введен в действие стандарт, определяющий как собственно TLS, так и использование в TLS отечественных криптографических алгоритмов. Рабочее название стандарта – BTLS.TLS является объединением нескольких субпротоколов, разбитых на два уровня. На нижнем уровне действует протокол Record, обеспечивающий шифрование и имитозащиту данных. На верхнем уровне действуют 3 протокола, основным из них является протокол Handshake. С помощью Handshake стороны согласуют применение определенных криптографических алгоритмов, формируют общий ключ, строят ключи для протокола Record, проводят аутентификацию друг друга. Применяемые алгоритмы оформляются в TLS в виде криптонабора (cipher suite). В TLS предусмотрено расширение перечня криптонаборов и методов аутентификации сторон.

BTLS определяет следующие семейства дополнительных криптонаборов:

– RDPFOK_WITH_GOST – два криптонабора на основе алгоритмов ГОСТ 28147 (шифрование, имитозащита), СТБ 1176.1 (хэширование), СТБ 1176.2 (ЭЦП) и протоколов формирования общего ключа в простых полях, определенных в [2];

– BIGN_WITH_BELT – девять криптонаборов на основе алгоритмов СТБ 34.101.31 (шифрование, имитозащита, хэширование), СТБ 34.101.45 (ЭЦП, транспорт ключа).

Криптонаборы RDPFOK_WITH_GOST были рассмотрены в [3]. В работе рассматриваются новые криптонаборы BIGN_WITH_BELT и связанные с ними методы аутентификации.

Криптонаборы

Криптонабор определяет, какие алгоритмы шифрования, имитозащиты, генерации псевдослучайных данных и формирования общего ключа будут использоваться в сессии TLS.

Алгоритмы шифрования. В TLS могут использоваться алгоритмы шифрования трех типов: поточные алгоритмы, блочные алгоритмы и алгоритмы одновременного шифрования и имитозащиты (AEAD-алгоритмы в обозначениях [1]). В криптонаборах BIGN_WITH_BELT поддержаны все эти типы:

– алгоритм шифрования СТБ 34.101.31 в режиме счетчика (belt-ctr) используется в качестве поточного;

– алгоритмы шифрования СТБ 34.101.31 в режиме сцепления блоков (belt-cbc) используются в качестве блочных;

– алгоритмы одновременного шифрования и имитозащиты СТБ 34.101.31 (belt datawrap) используются как AEAD-алгоритмы.