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.

Алгоритм имитозащиты. В TLS данные, зашифрованные с помощью поточных или блочных алгоритмов, должны сопровождаться имитовставками. В BIGN_WITH_BELT в необходимых случаях применяется алгоритм вычисления имитовставки, определенный в СТБ 34.101.31 (belt-mac).

Алгоритм генерации псевдослучайных данных. В TLS алгоритм генерации псевдослучайных чисел (PRF-алгоритм в обозначениях [1]) используется для построения ключей и синхропосылок, а также для верификации сообщений протокола Handshake. Стандартный PRF-алгоритм последней редакции TLS строится на основе алгоритма HMAC, который, в свою очередь, строится на некотором алгоритме хэширования. Во всех криптонаборах BIGN_WITH_BELT используется стандартный PRF-алгоритм с алгоритмом хэширования СТБ 34.101.31 (belt-hash).

Алгоритмы формирования общего ключа. В протоколе TLS имеется определенная свобода выбора алгоритма (или, точнее, механизма) формирования общего ключа. Тем не менее, в [1] описаны четыре типа таких алгоритмов, которые применяются в большинстве существующих на сегодняшний день решений. Алгоритмы двух типов не обеспечивают защиту от атак типа «противник посередине» и «чтение назад». Поэтому в BTLS были включены алгоритмы только двух оставшихся типов:

– dht-bign – транспорт ключа на основе СТБ 34.101.45 (bign-keytransport);

– dhe-bign – протокол Диффи – Хэллмана с эфемерными ключами, которые подписываются с помощью алгоритмов СТБ 34.101.45 (bign-sign).

Дополнительно в BTLS определен алгоритм формирования общего ключа, соответствующий RFC 4279 [4]:

– dht-psk-bign – транспорт ключа типа DHT_BIGN с использованием предварительно распределенных общих секретов.

В перечисленных алгоритмах формирования общего ключа используется сертификат сервера с открытым ключом СТБ 34.101.45 (bign-pubkey).

Обязательный криптонабор. Любая реализация BTLS должна поддерживать криптонабор с алгоритмом шифрования belt-ctr, алгоритмом имитозащиты belt-mac и алгоритмом формирования общего ключа dht-bign. Поддержка остальных 8 криптонаборов является необязательной.

Методы аутентификации

Аутентификация в BTLS основана на проверке действительности сертификатов открытых ключей сторон и на проверке знания сторонами соответствующих личных ключей. Для криптонаборов с алгоритмом формирования общего ключа dht-psk-bign дополнительная аутентификация состоит в проверке знания общего секрета (предполагается, что этот секрет был надежно передан сторонам протокола, подлинность которых была предварительно проверена). При аутентификации используются сертификаты, в которых фиксируются открытые ключи алгоритмов СТБ 34.101.45 (bign-pubkey).

Аутентификация сервера. В протоколе Handshake сервер передает клиенту сертификат, который при использовании алгоритма dhe-bign содержит открытый ключ электронной цифровой подписи, а при использовании алгоритмов dht-bign и dht-psk-bign – открытый ключ транспорта. Последующее успешное завершение Handshake означает, что аутентификация сервера проведена успешно.

Аутентификация клиента. В протоколе Handshake сервер запрашивает у клиента его сертификат. В этом запросе указываются возможные типы сертификатов, который должен предоставить клиент, а также типы пар (алгоритм хэширования, алгоритм ЭЦП), которые разрешается использовать при проверке подписи сертификата. Разрешается использовать сертификаты открытых ключей типа bign-pubkey и пару алгоритмов (belt-hash, bign-sign). Сервер может запросить сертификат клиента только после предъявления своего сертификата. Успешное завершение Handshake означает, что аутентификация клиента проведена успешна.

Литература:

1. Dierks, T. The Transport Layer Security (TLS) Protocol. Version 1.2. RFC 5246 / T. Dierks, E. Rescorla. – August, 2008.

2. Проект руководящего документа Республики Беларусь «Банковские технологии. Протоколы формирования общего ключа». – Минск, 1997.

3. Маслов, А.С. Криптонаборы протокола TLS, основанные на отечественных криптографических алгоритмах / А.С. Маслов, С.В. Агиевич, А.В. Федин, Д.В. Шпилевский // Информационные системы и технологии (IST'2010): Материалы VI Междунар. Конф. (Минск, 24-25 ноября 2010 г.). – Минск: А.Н. Вараксин, 2010. – С. 65–68.

4. Eronen, P. Pre-Shared Key Ciphersuites for TLS. RFC 4279 / P. Eronen, H. Tschofenig. – December, 2005.

Abstract

The TLS protocol is under standardization in Republic of Belarus. The future standard will include additional TLS ciphersuites based on domestic cryptographic algorithms. In this paper we describe additional suites and related authentication methods.

Поступила в редакцию 18.05.2013 г.

СТЕГАНОГРАФИЯ: МОДЕЛИ И МЕТОДЫ ОЦЕНКИ НАДЕЖНОСТИ

УДК 519.2

Ю.С. Харин, Е.В. Вечерко,
НИИ ППМИ БГУ, г. Минск

Аннотация

В статье рассматриваются математические модели вкрапления, возникающие в задачах стеганографии. На основе марковских моделей контейнеров, среднеквадратических ошибок оценивания уровня вкрапления и вероятностей ошибок при проверке гипотез о факте вкрапления построены оценки надежности. Представлены результаты компьютерных экспериментов.

Введение

Стеганография имеет целью сокрытие сообщений в открытых цифровых данных, называемых контейнерами.