СПОСОБ РАССЫЛКИ ЗАЩИЩЕННЫХ ДАННЫХ С РЕГУЛИРОВАНИЕМ ДОСТУПА К ОТДЕЛЬНЫМ ИХ РАЗДЕЛАМ

Лебедев А.Н.[1]

Предлагается новый способ рассылки защищенных данных в электронной форме по общедоступным открытым каналам электросвязи, позволяющий точно регулировать моменты доступа получателей рассылаемых данных к отдельным их разделам даже после момента рассылки. При этом достигается защита конкретной порции данных от тех получателей, которым данная порция не предназначена, даже если среди произвольной группы таких получателей данных произойдет сговор. Для обеспечения надежности защиты передаваемых данных получатели снабжаются специальными принтерами, обладающими "интеллектуальным" встроенным микропроцессорным блоком управления, который управляется упрощенной операционной системой, что служит защитой его от воздействия вредоносного программного обеспечения (вирусов, троянов, компьютерных червей и т.п.) даже при подключении через локальную компьютерную сеть к сети интернет без дополнительной защиты в виде сетевых экранов или VPN–серверов. Кроме того, каждый пользователь системы рассылки имеет специальный персональный компактный аппаратный модуль (токен), который подключается к принтеру через USB–порт и может производить все криптографические преобразования информации, связанные с реализацией технологии электронной подписи и шифрования данных непосредственно в защищенной памяти токена.

***Ключевые слова**: рассылка защищенных данных, регулирование доступа, криптографические преобразования, генерация ключей, электронная подпись, хэширование, шифрование, токен, интеллектуальный принтер*

Введение. Современная криптография позволяет очень эффективно решать многие практические задачи, решение которых до сегодняшнего дня требовало слишком больших материальных и человеческих затрат, если было вообще возможно.

Наглядным и наиболее широко известным примером может служить протокол Диффи-Хеллмана – протокол выработки общего секрета произвольной парой удаленных пользователей сети интернет без предварительного непосредственного контакта между ними, а только посредством обмена открытыми для всех посылками (пакетами данных) по общедоступным каналам связи [1, 2].

Другими не менее широко известными примерами служат алгоритм шифрования с открытым ключом – алгоритм RSA [1, 2], а также стандартизованные в РФ алгоритмы электронной подписи ГОСТ Р 34.10–94, ГОСТ Р 34.10–2001 и ГОСТ Р 34.10-2012 и национальные стандарты цифровой подписи США DSA – 1995 и ECDSA – 2001.

Новое поколение электроники. Современный тренд развития рынка дистанционных электронных услуг состоит в том, что для удобства их потребления пользователи все шире используют свои персональные мобильные устройства (ПК, планшеты, смартфоны и т. п.).

В корпоративной среде несколько лет назад появился и стал весьма распространенным так называемый принцип BYOD (от английского Bring Your Own Device), когда сотрудники компаний используют свои персональные электронные устройства для выполнения служебных заданий и обязанностей [3, 4, 7].

При таком подходе достигается заметное сокращение расходов компании на приобретение и поддержание эксплуатации электронных устройств для выполнения сотрудниками действий, связанных с выполнением обмена информацией при осуществлении бизнес - процедур.

Но одновременно с этим заметно возрастают риски, связанные с возможностью утечки важной или даже конфиденциальной коммерческой и технической информации, а также персональных данных сотрудников корпорации при передаче ими информации по открытым каналам общедоступных сетей с использованием персональных электронных устройств общего назначения [3, 4].

В качестве панацеи от этой опасности обычно считается применение криптографических методов защиты данных при их передаче по каналам общедоступных массовых сетей. Однако, опыт последних лет, в частности, информация, раскрытая бывшим сотрудником АНБ США Эдвардом Сноуденом [5, 6], показывает, что криптография сама по себе еще не гарантирует надежную защиту данных.

В частности, даже при использовании для защиты данных самых надежных современных алгоритмов

1 Лебедев Анатолий Николаевич, старший научный сотрудник, кандидат физико-математических наук, МГТУ им. Н.Э. Баумана, Москва, lan@lancrypto.com

шифрования и распределения ключей, а для строгой аутентификации данных – алгоритмов электронной подписи, но при реализации этих алгоритмов в виде программных модулей для компьютера или смартфона, возможны практически эффективные атаки на такую защиту посредством вирусов, троянов или другого так называемого «вредоносного ПО».

Поэтому для ситуаций, в которых защита данных, передаваемых по каналам связи, играет особенно важную роль, к таковым относятся системы ДБО, электронных торгов, электронных платежей и т. п., реализация криптографических преобразований выносится на отдельные защищенные аппаратные модули: токены, смарт-карты, HSM-модули и т. д. [7].

Способ защищенной рассылки данных. Мы рассмотрим одну актуальную практическую задачу: обеспечить центру (центрам) возможность рассылки важной и закрытой от посторонних глаз информации большому числу удаленных получателей по открытым каналам электросвязи таким образом, чтобы он мог точно и относительно просто регулировать моменты доступа конкретного получателя к конкретным разделам полученной от этого центра рассылки информации. Причем регулировать так, чтобы никакими усилиями любых объединенных групп получателей невозможно было получить доступ к тем разделам уже полученных пользователями данных, доступ к которым им еще не предоставлен центром рассылки.

В такой постановке простым и на первый взгляд достаточно хорошим решением выглядит такое, при котором на сервере центра рассылки и на компьютерах получателей устанавливаются программы электронной подписи и шифрования данных, в комплект последних включаются модули формирования общего ключа шифрования между центром и конкретным пользователем по протоколу Диффи-Хеллмана. Каждый такой общий ключ служит для шифрования отдельной порции данных, передаваемых центром конкретному получателю (обычно его называют сессионным ключом).

Однако такое решение неудовлетворительно по целому ряду показателей. Во-первых, пользователь может непосредственно по получении блока данных его расшифровать, во-вторых, на компьютере массового пользователя (если это рядовой пользователь сети интернет) практически невозможно обеспечить доверенную среду работы программ электронной подписи и шифрования данных, а это может привести к взлому всей системы защиты [3, 4, 5].

Поэтому мы в качестве практического решения поставленной задачи предлагаем следующий способ (последовательность действий) рассылки защищенных данных по открытым каналам связи со строгим регулированием доступа получателей к конкретному блоку данных:

– в качестве приемных устройств получателей («приемников») используются не компьютеры, а более простые специализированные устройства, которые допускают возможность подключения компактных внешних аппаратных криптографических модулей (токенов или смарт-карт), реализующих в защищенной памяти все необходимые криптографические преобразования: генерацию ключевых пар («закрытый – открытый» ключи), хэширование данных, создание и проверка электронных подписей, шифрование данных;

– пользователи в защищенной памяти своих персональных токенов генерируют ключевые пары для ЭП и шифрования;

– открытые ключи пользователей для ЭП и шифрования регистрируются центром рассылки (достоверность получателя проверяется при его визите в центр рассылки или к доверенному уполномоченному регистратору);

– центр генерирует ключевую пару для ЭП и ключевые пары шифрования для каждого пользователя и каждого отдельно трактуемого блока данных;

– центр записывает в память токенов пользователей свой открытый ключ проверки ЭП;

– для шифрования конкретного блока данных для конкретного получателя центр формирует парный ключ шифрования*) по протоколу Диффи-Хеллмана, подписывает блок данных своей ЭП, шифрует на ключе шифрования данного блока для данного пользователя;

– центр передает данные пользователям по общедоступным каналам связи;

– в момент предоставления доступа конкретного пользователя к конкретному блоку данных центр передает по открытым каналам открытый ключ шифрования данного блока;

– при смене ключей в регулярном режиме пользователи отправляют в центр свой новый открытый ключ шифрования данных зашифрованным на действующем парном ключе шифрования данных; *)

– в случае компрометации ключей шифрования данных *) пользователя он может отправить в центр новый открытый ключ шифрования данных подписанным его ЭП;

– в случае компрометации также и ключей ЭП пользователя он должен повторить все перечис-

*) Возможный вариант: центр формирует парный с данным пользователем ключ для шифрования ключей шифрования данных для этого конкретного пользователя, а уже на этом ключе шифрует и передает пользователю зашифрованные ключи шифрования данных.

ленные действия, включая физический контакт с центром, заново.

Различные конкретные варианты данного способа могут применяться с различными конкретными типами устройств, называемых в общей схеме метода «приемником». Это могут быть принтеры, офисные центры или другие специализированные устройства, ограниченная функциональность которых служит защитой от вирусов, троянов и других атак по сети интернет. Суть предлагаемого способа от этого не зависит.

Детальное описание способа предполагается дать в отдельной статье и заявке на изобретение.

Рецензент: Матвеев Валерий Александрович, доктор технических наук, профессор, v.a.matveev@bmstu.ru

Литература:

1. Diffie W., Hellman M., New Directions in Cryptography // IEEE Transactions in Information Theory, 22, 5 (1976), p. 644-654.
2. Schneier B., Applied Cryptography - Protocols, Algorithms, and Source Codes in C, 2nd Edition, John Wiley & Sons, 1996.
3. Лебедев А.Н. Электронная подпись: новый этап // Вестник Московского городского педагогического университета. Серия: Экономика. 2013. № 1 (20). С. 43-51.
4. Лебедев А.Н. Криптографические примитивы. Асимметричные шифры. В кн. Математические основы информационной безопасности / Басараб М.А., Булатов В.В., Булдакова Т.И. и др.; Под ред. В.А.Матвеева. М.: НИИ радиоэлектроники и лазерной техники, 2013. С. 214-228.
5. National Security Agency, Fact Sheet NSA Suite B Cryptography, archived on 22 March 2010, URL: https://web.archive.org/web/20100322225318/.
6. National Security Agency, Cryptography today, August 2015, URL: www.nsa.gov/ia/programs/suiteb_cryptography.
7. Рибер Г., Малмквист К., Щербаков А. Многоуровневый подход к оценке безопасности программных средств // Вопросы кибербезопасности. 2014. № 1 (2). С. 36-39.

SECURED DATA DISTRIBUTION METHOD WITH REGULATED ACCESS OF RECIEVERS TO THE DATA SENT

Lebedev A.N.[2]

We propose a new method of secured electronic data distribution via public networks with a strong regulated access of the data receivers not only in distribution process period of time, but as long as it needed afterward. The method gives to a sending center an ability to regulate access of any user to any particular data block or a message sent to this user not only before the sending or in the process of the sending, but as long afterwards, as the center needs. To protect any secured data block from any combination of users without the legal receiver of the block.

Any user of the system have to have a personal bearable hardware device (called token) that is able to implement cryptographic data protection mechanisms just in their protected memory store and may be connected to the user's printers immediately through a USB port. The method gives an opportunity to securely protect any sensitive data even for the insecure environment on a user computer or a local server. All cryptographic transformations are executed just in secure token memory and cryptographic keys are generated and stored securely in this memory too.

Keywords*: secured data distribution, access regulation, cryptographic transformations, cryptographic key generation and store, digital (electronic) signature, hash function, token, intelligent printer*

References:

1. Diffie W., Hellman M., New Directions in Cryptography, IEEE Transactions in Information Theory, 22, 5 (1976), p. 644-654.
2. Schneier B., Applied Cryptography - Protocols, Algorithms, and Source Codes in C, 2nd Edition, John Wiley & Sons, 1996.
3. Lebedev A.N. Elektronnaya podpis': novyy etap, Vestnik Moskovskogo gorodskogo pedagogicheskogo universiteta. Seriya: Ekonomika. 2013. No 1 (20), pp. 43-51.
4. Lebedev A.N., Kriptograficheskie primitivy. Asimmetrichnye shifry. V kn. Matematicheskie osnovy informatsionnoy bezopasnosti, Basarab M.A., Bulatov V.V., Buldakova T.I. and etc, pod red. V.A.Matveeva. Moscow: NII radioelektroniki i lazerno tekhniki, 2013, pp. 214-228.
5. National Security Agency, Fact Sheet NSA Suite B Cryptography, archived on 22 March 2010, URL: https://web.archive.org/web/20100322225318/.
6. National Security Agency, Cryptography today, August 2015, URL: www.nsa.gov/ia/programs/suiteb_cryptography.
7. Riber G., Malmkvist K., Shcherbakov A. Mnogourovnevyy podkhod k otsenke bezopasnosti programmnykh sredstv, Voprosy kiberbezopasnosti. 2014. No 1 (2), pp. 36-39.

2 Anatoliy Lebedev, Associate Professor, Ph.D. (Math), Bauman Moscow State Technical University, Moscow, lan@lancrypto.com