УДК 004.056.55 Вестник УрФО № 2(36) / 2020, с. 24–28

Зырянова Т. Ю., Распопов Н. А.

DOI: 10.14529/secur200204

РЕАЛИЗАЦИЯ ПРОТОКОЛА ДИФФИ–ХЕЛЛМАНА В НЕЗАЩИЩЁННОМ ОТ ПЕРЕХВАТА КАНАЛЕ

В статье рассматривается реализация протокола Диффи–Хеллмана в незащищённом от перехвата канале. Суть данного метода заключается в применении стеганографии для передачи открытого ключа в незащищённом канале передачи данных. Открытый ключ зашифровывается при помощи блочного шифра и встраивается в изображение стеганографическим методом LSB. Уникальность изображения и невозможность изменения ключа обеспечивается за счёт лавинного эффекта. Реализация протокола Диффи–Хеллмана в незащищённом канале передачи данных уже давно остаётся актуальной, хотя и существует решение с использованием технологии инфраструктуры открытых ключей. В статье предложено новое решение данной проблемы.

Ключевые слова: *асимметричная криптография, блочное шифрование, инфраструктура открытых ключей, незащищённый канал, протокол Диффи–Хеллмана, стеганография.*

Zyryanova T. Yu., Raspopov N. A.

IMPLEMENTATION OF THE DIFFIE-HELLMAN PROTOCOL IN A CHANNEL UNLESS PROTECTED FROM INTERCEPT

This article discusses the implementation of the Diffie-Hellman protocol in an unprotected channel. The essence of this method is to use steganography to transmit the public key in an unsecured channel. The public key is encrypted using a block cipher and encoded into the picture using the LSB method. The uniqueness of the picture and the impossibility of changing the key is ensured by the avalanche effect. The implementation of the Diffie-Hellman protocol in an insecure channel has long remained relevant, although there is a solution in the form of public key infrastructure, but in this article a new solution to this problem was proposed.

Keywords: *asymmetric cryptography, block encryption, Diffie-Hellman protocol, public key infrastructure, steganography, unprotected channel.*

В 1974 году Уитфилд Диффи и Мартин Хеллман решили проблему, остро стоявшую перед криптографией – безопасное распределение ключей шифрования. На тот момент не существовало метода, который позволил бы вырабатывать общий ключ для его использования в симметричной системе шифрования. Данный протокол основан на эксплуатации задачи вычисления дискретного логарифма[1].

При работе алгоритма каждый пользователь:

1. Генерирует случайное натуральное число a – закрытый (или секретный) ключ;

2. Совместно с другим пользователем устанавливает открытые параметрыри g (обычно значения p и g генерируются на одной стороне и передаются другой), где

• p является случайным простым числом,

• (p – 1)/ 2 также должно быть случайным простым числом (для повышения безопасности),

• g является первообразным корнем по модулю p (также является простым числом);

3. Вычисляется открытый ключ A, используя преобразования над закрытым ключом: $A = g^a mod p$;

4. Обменивается открытыми ключами с удалённой стороной.

5. Вычисляет общий секретный ключ K, используя открытый ключ удалённой стороны B и свой закрытый ключ a: $K = B^A mod p$.

Ключ получается равным с обеих сторон, потому что: $B^a \bmod p = (g^b \bmod p)^a \bmod p = g^{ab} \bmod p = (g^a \bmod p)^b \bmod p = A^b \bmod p$. В практических реализациях в качествеаи b используются числа порядка 10^{100} и рпорядка 10^{300}. Число gнеобязательно должно быть большим и обычно имеет значение в пределах первого десятка.

Протокол Диффи–Хеллмана позволил решить проблему распределения ключей, но, как и у всего, у него есть недостатки. Таким недостатком является то, что невозможно однозначно установить, является ли открытый ключ, который был получен в ходе реализации протокола легальным, а не подменённым злоумышленником. Именно поэтому данный протокол уязвим к атаке «человекпосередине». Суть атаки «человекпосередине» или MITM (Men-in-the-middle) заключается в том, что злоумышленник получает возможность не только читать весь поток передаваемых сообщений, но и осуществляет вмешательство в протокол передачи, удаляя или искажая информацию (рис. 1). Злоумышленник тайно ретранслирует и при необходимости изменяет связь между сторонами. Данная атака особенно опасна тем, что практически незаметна для пользователей. Пользователи сети могут даже не догадываться, что весь сетевой трафик проходит через злоумышленника.

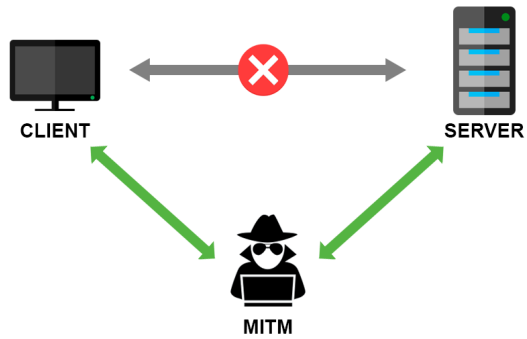

Рис. 1. Реализация атаки «человекпосередине»

Атака обычно начинается с прослушивания канала связи и заканчивается тем, что криптоаналитик пытается подменить перехваченное сообщение, извлечь из него полезную информацию, перенаправить его на какой-либо внешний ресурс. Предположим, Алиса планирует передать Бобу информацию. Злоумышленник Ева обладает знаниями о структуре и свойствах используемого метода передачи данных, а также о факте планируемой передачи информации, которую она планирует перехватить. Для совершения атаки Ева «представляется» Алисе Бобом, а Бобу как Алиса. Алиса, ошибочно думая, что ведёт обмен информацией с Бобом, на самом деле посылает данные Еве. Ева в своём случае совершает манипуляции с перехваченной информацией (скопировав, модифицировав) пересылает её Бобу; Боб в своём случае полагает, что данная информация пришла от Алисы. Одним из примеров атак типа «человек посередине» является активное прослушивание, при котором злоумышленник устанавливает независимые связи с жертвами и передаёт сообщения между ними. Тем самым он заставляет жертв поверить, что они разговаривают непосредственно друг с другом через частную связь, фактически же весь разговор управляется злоумышленником. Злоумышленник должен уметь перехватывать все передаваемые между двумя жертвами сообщения, а также вводить новые. В большинстве случаев это довольно просто, например, злоумышленник может вести себя как «чело-

век посередине» в пределах диапазона приёма беспроводной точки доступа (Wi-Fi).

На сегодняшний день известно решение данной проблемы – это инфраструктура открытых ключей PublicKeyInfrastructure (PKI) [2]. Основная идея PKI заключается в том, что удостоверяющий центр создает электронный документ — сертификат открытого ключа, таким образом удостоверяя факт того, что закрытый (секретный) ключ известен эксклюзивно владельцу этого сертификата, а открытый ключ (publickey) свободно передается в сертификате. Недостатком данной системы является то, что сертификат может быть скомпрометирован, и тогда злоумышленник сможет под видом легального пользователя отправлять сообщения получателю. PKI позволяет нейтрализовать уязвимость протокола Диффи–Хеллмана, но это решение является слишком громоздким, так как оно ставит между абонентами удостоверяющий центр, который даёт гарантию, что ключ, полученный абонентом является легальным. Наличие третьей стороны, принимающей участие в обмене информации, увеличивает её стоимость. PKI помогает обойти уязвимость протокола Диффи–Хеллмана, но она не решает эту проблему полностью. Инфраструктура открытых ключей помогает только тем, кто готов платить за сертификат. На сегодняшний день необходима альтернатива PKI, так как сфера информационных технологий развивается бурными темпами, и необходимо решение, которое не будет ставить абонентов в зависимость от третьей стороны. В статье предлагается метод решения проблемы уязвимости данной технологии к атаке MITM. Предлагаемое решение совмещает в себе стеганографические и криптографические методы.

Научная новизна предлагаемого метода обусловлена нестандартным подходом к использованию криптографии и стеганографии. В данном случае шифрование используется как средство, придающее уникальность выбранному ключу. Придание уникальности обеспечивается за счёт «лавинного эффекта». Стеганографическая часть протокола также используется нестандартным образом. В данном случае при помощи стеганографии мы будем кодировать зашифрованный ключ методом RGB. Это позволит получить изображение с уникальной палитрой цветов.

Обозначим предполагаемых санкционированных участников обмена сообщениями как Алиса и Боб, а в качестве злоумышленника будет выступать Ева.

Предлагаемый алгоритм включает следующие этапы.

1. Алиса и Боб вырабатывают открытые ключи в соответствии с протоколом Диффи – Хеллмана.

2. Алиса и Боб выбирают ключи для шифрования шифром AES и публикуют их как открытую информацию. Данные ключи могут не совпадать, так как в этом случае шифрование используется исключительно для реализации «лавинного эффекта».

3. Алиса и Боб встраивают ключи в контейнер, который вмещает в себя ключ выбранной длины. Изображение-контейнер с встроенными ключами также публикуется как открытая информация. «Лавинный эффект» обеспечивает уникальность полученного изображения, и малейшие изменения в ключе приведут к сильному искажению изображения.

4. Алиса и Боб обмениваются изображениями.

5. Алиса и Боб сравнивают полученные изображения с изображением, опубликованным ранее и, если изображения совпадают, то переходят к следующему этапу. Сравнение изображений происходит при помощи сканирования структуры изображений, полученных методом RGB. Если существует различие хотя бы в 1 байт, то изображение считается скомпрометированным и соединение разрывается. Данная процедура может считаться также барьером защиты. Злоумышленнику необходимо будет подобрать изображение идентичное изображению Алисы и Боба. Эта процедура подбора подобна поиску коллизий 2 рода хэш-функции второго рода.

6. Алиса и Боб декодируют изображение и расшифровывают свои открытые ключи при помощи ранее опубликованных ключей AES.

7. Алиса и Боб вырабатывают общий ключ, следуя протоколу Диффи–Хеллмана.

Обобщённая модель алгоритма представлена на рис. 2.

В случае перехвата Евой изображения с встроенным в него ключом, она сможет лишь раскодировать изображение и получить открытый ключ, но, чтобы заменить его на свой, ей будет необходимо потратить значительное количество времени на подбор такого ключа, который при кодировании будет давать изображение, идентичное изображению

Рис. 2. Реализация алгоритма

Алисы и Боба. Так же злоумышленнику необходимо скомпрометировать два изображения, а это увеличивает время работы в два раза. Обмена сообщениями между Алисой и Бобом происходит за относительно небольшой промежуток времени, любая задержка в момент обмена сообщениями может выдать злоумышленника. Это делает атаку нецелесообразной для злоумышленника, так как затраты на атаку начнут превышать её стоимость и как следствие утратится целесообразность атаки. Также данная атака будет требовать значительного количества времени или же больших вычислительных ресурсов.

Преимущество данного алгоритма заключается в том, что пользователи являются независимыми от центров сертификации. Пользователям достаточно использовать предлагаемый алгоритм, для того чтобы выработать общий ключ. Также данный алгоритм применим в сетях, которые не используют интернет, так как в данном случае единственное, что необходимо двум абонентам для выработки общего ключа – это канал связи. Именно поэтому данный алгоритм может найти место применение в военной сфере. Алгоритм не обладает данными, которые необходимо держать в секрете. Это исключает вероятность несанкционированной утечки информации и облегчает работу с ней. Также в качестве достоинства предложенного решения можно выделить его относительную простоту. Это позволяет упростить порог квалификации, необходимой для эксплуатации данного решения. В принципе реализацию данного алгоритма может использовать любой человек, имеющий базовые познания в криптографии. Стоит отметить, что такой протокол является легко масштабируемым, так как при выработке не имеет ограничительных мер.

Если рассматривать финансовую сторону, то данный протокол является менее затратным вариантом в сравнении с сертификатами, которые необходимо продлевать по истечению срока. Он позволяет увеличить количество интернет-ресурсов, которые будут использовать защищённое соединение, так как потребует лишь небольшого увеличения вычислительных мощностей сервера. Это гораздо выгоднее, нежели использовать сертификат. Это открывает сектор коммерческих организаций. Данный алгоритм предлагает более выгодные условия для рынка, нежели сертификаты. Предложенный вариант решения проблемы реализации протокола Диффи–Хеллмана в незащищённом от перехвата канале предлагает необычный взгляд на использование криптографических и стеганографических примитивов, так как в данном случае шифрование не используется для обеспечения конфиденциальности, а кодирование стегонтейнера не используется для сокрытия факта передачи информации. Шифрование позволяет обеспечить невозможность внесения изменений в ключ или его полной замены, кодирование позволяет придать данному ключу оболочку в виде изображения.

С точки зрения производительности данный алгоритм несильно отличается от обычного варианта алгоритма Диффи–Хеллмана. Все операции не являются вычислительно сложными, единственное, что может составить задержку – это проверка изображения при получении. Данный алгоритм реализуем на таких объектно-ориентированных языках программирования как C#.

Область применения данного метода довольно обширна. Любая система, которая требует шифрования потока сообщений между двумя абонентами, может использовать его в своей деятельности. В частности, винтернет-пространстве любой информационный ресурс, использующий технологию https может использовать данный алгоритм для организации защиты информации. Также алгоритм подходит для реализации частной пе-

переписки в мессенджерах. Например, данная функция может использоваться в качестве дополнительного шифрования переписки. Если пользователи считают, что их переписка может попасть не в те руки и хотят обезопасить себя и свои данные, то предложенный алгоритм является адекватным решением. Он позволит пользователям генерировать персональный ключ шифрования, который будет известен только им. Это позволит обеспечить конфиденциальность информации. В том числе данный протокол может найти своё применение в прикладных программах, направленных на защиту информации. Он позволит упростить процедуру генерации общего ключа на основе протокола Диффи–Хеллмана, если компания не может обеспечить защиту канала передачи информации. Это в свою очередь позволит снизить затраты на обеспечение информационной безопасности или же усилить уязвимые места в системе безопасности.

Если рассматривать протокол с точки зрения злоумышленника, то потенциальными уязвимостями могут быть изображения, полученные входе кодирования зашифрованного открытого ключа. Если будет найден алгоритм, который за полиномиальное время позволит получать идентичное изображение, но с другим встроенным ключом, то данный алгоритм можно будет считать скомпрометированным. В остальных случаях он является хорошим сдерживающим фактором для злоумышленника, так как для реализации атаки требуется значительное количество вычислительных ресурсов и высокий уровень квалификации.

В данной статье был предложен новый метод решения проблемы реализации протокола Диффи–Хеллмана в незащищённом от перехвата канале. Также был предложен нестандартный взгляд на криптографические и стеганографические примитивы. В итоге был получен алгоритм, не требующий высокой вычислительной мощности со стороны пользователей и являющийся простым в использовании. Были рассмотрены сферы применения, где данный алгоритм может применяться и успешно доказывать свою эффективность в сравнении с PKI.

Литература

1. ДиффиУ., Хеллман М.Новые направления в криптографии. IEEETransactionsonInformationTheory, vol. IT-22, Nov. 1976, pp: 644—654.

2. Горбатов В. С., Полянская О. Ю. Основытехнологии PKI. – М.: Горячаялиния – Телеком, 2003.

References

1. Diffi U., Khellman M. Novyye napravleniya v kriptografii. IEEETransactionsonInformationTheory, vol. IT-22, Nov. 1976, pp: 644—654.

2. GorbatovV. S., PolyanskayaO. YU. Osnovytekhnologii PKI. – M.: Goryachayaliniya – Telekom, 2003.

ЗЫРЯНОВА Татьяна Юрьевна, доцент кафедры «Информационные технологии и защита информации» Уральского государственного университета путей сообщения, кандидат технических наук. 620034, г. Екатеринбург, ул. Колмогорова, д. 66. E-mail: tzyryanova@usurt.ru

РАСПОПОВ Никита, студент 2 курса электротехнического факультета по направлению подготовки Информационная безопасность Уральского государственного университета путей сообщения. 620034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: nastyazavedenskaya@yandex.ru

ZYRYANOVA Tatiana Yuryevna, associate professor of Department «Information Technology and Information Security» of the Ural State University of Railway Transport. Bld. 66, Kolmogorovastr., Yekaterinburg, 620034. E-mail: tzyryanova@usurt.ru.

RASPOPOV Nikita, 2-yearstudentof Department «Information Technology and Information Security» of the Ural State University of Railway Transport. Bld. 66, Kolmogorovastr., Yekaterinburg, 620034. E-mail: wildpro6@gmail.com