УДК 004.056.(075.8) DOI:10.31854/1813-324X-2021-7-3-79-90

Способ аутентификации значений Диффи – Хеллмана на основе предварительно распределенных случайных последовательностей и алгоритма аутентификации Вегмана – Картера с одноразовым ключом

В.А. Яковлев[1*]

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
*Адрес для переписки: viyak@bk.ru

Информация о статье
Поступила в редакцию 09.06.2021
Принята к публикации 19.07.2021

Ссылка для цитирования: Яковлев В.А. Способ аутентификации значений Диффи – Хеллмана на основе предварительно распределенных случайных последовательностей и алгоритма аутентификации Вегмана – Картера с одноразовым ключом // Труды учебных заведений связи. 2021. Т. 7. № 3. С. 79–90. DOI:10.31854/1813-324X-2021-7-3-79-90

Аннотация: *Исследуется способ аутентификации ключей, формируемых методом Диффи – Хеллмана, в условиях применения злоумышленником атаки «человек-посередине». Предполагается, что пользователи Алиса и Боб, формирующие ключ, имеют предварительно распределенные случайные цепочки бит a и b соответственно, полученные либо от некоторого источника, либо сгенерированные ими самими на основе данных, полученных от магнитометров или акселерометров из состава мобильных устройств. Злоумышленник не имеет доступа к этим цепочкам. Предложен способ аутентификации значений Диффи – Хеллмана (DH-значений). С этой целью сообщение (DH-значение) Алисой разделяется на N блоков. Для каждого блока вычисляется аутентификатор с использованием алгоритма Вегмана – Картера с одноразовым ключом, в качестве которого используются последовательности a и b. DH-значение и аутентификаторы передаются по каналу Бобу, который вычисляет аутентификаторы от принятого DH-значения и сравнивает их с аутентификаторами, принятыми из канала. Если число не аутенифицированных блоков не превышает установленный порог, то аутентификация DH-значения считается успешной. Особенность решения данной задачи состоит в том, что последовательности a и b в точности не совпадают. Выведены соотношения для оценивания вероятности ложного отклонения DH-значения (из-за несовпадения цепочек a и b) и вероятности навязывания ложного DH-значения.*
Проведена оптимизация параметров способа (количества подблоков и длины аутентификатора), при которых минимизируется расход ключа аутентификации (цепочек a и b) при выполнении заданных требований по вероятности подмены и вероятности ложного отклонения DH-значения. Приведены примеры выбора параметров аутентификации DH-значения длиной 256 бит. Показана возможность обеспечения достаточно малых значений вероятности ложного отклонения DH-значения и вероятности навязывания ложного DH-значения (10^6).

Ключевые слова: *метод Диффи – Хеллмана, аутентификациа, униферсальные хэш-функции, аутентификация Вегмана – Картера.*

Введение

Метод Диффи – Хеллмана [1] позволяет использовать незащищенный от перехвата канал связи для формирования общего ключа шифрования с целью создания безопасного соединения между двумя корреспондентами. Этот метод нашел широкое применение в сетевых протоколах SSL/TLS, IPsec, PGP и др. Суть метода следующая. Пользователи сети Алиса (A) и Боб (B) согласуют параметры: p и g, где p – простое число, а g – элемент конечного поля $GF(p)$, порождающий группу, имею-

щую большой порядок, и выполняют следующий протокол:

– Алиса генерирует элемент поля $x \in (1, p-1)$, вычисляет $X = g^x (\mathrm{mod} p)$ и посылает его Бобу;

– Боб генерирует элемент $y \in (1, p-1)$, вычисляет $Y = g^y (\mathrm{mod} p)$ и посылает его Алисе;

– Алиса вычисляет ключ $K = Y^x (\mathrm{mod} p)$;

– Боб вычисляет ключ $K = X^y (\mathrm{mod} p)$.

Легко видеть, что ключи, вычисленные Алисой и Бобом, равны между собой $K = g^{yx} (\mathrm{mod} p) = g^{xy} (\mathrm{mod} p)$.

Будем далее величины *X, Y,* которые передаются по открытым каналам, называть *значениями Диффи – Хеллмана* (*DH*-значениями).

Однако известно, что данный метод подвержен атаке «человек посередине». Алиса и Боб могут оказаться в ситуации, при которой они установили связь с злоумышленником – Евой (E), которая Алисе выдает себя Бобом, а Бобу представляется Алисой. Поэтому для дальнейшей совместной работы Алисе и Бобу требуется аутентифицировать ключи, сгенерированные по методу Диффи – Хеллмана.

Одним из направлений решения задачи аутентификации ключа является цифровая подпись *DH*-значений удостоверяющим центром или самим пользователем. Проверка цифровой подписи осуществляется с использованием открытого ключа, распространяемого в сети посредством сертификата. Такой подход требует использования технологии PKI, что не всегда удобно для пользователей особенно мобильных сетей.

Другим подходом к решению задачи аутентификации ключа, распределяемого по методу Диффи – Хеллмана, является использование для аутентификации предварительно распределенных между пользователями двоичных последовательностей. Эти последовательности пользователи вырабатывают в ходе процедуры сопряжения своих мобильных устройств во время личной встречи [2–4]. Нарушитель в этот момент удален от пользователей и не получает доступа к сообщениям, которыми они обмениваются. Непосредственно использовать вырабатываемые последовательности в качестве ключа шифрования пользователи не могут, так как эти последовательности содержат определенный процент ошибок (несовпадений). В настоящей работе проводится исследование способа аутентификации *DH*-значений с использованием аутентифицирующих последовательностей независимо от способа их получения.

Сценарий сопряжения мобильных устройств и аутентификация DH-значений

Задача получения пользователями идентичных последовательностей может быть решена на основе создания между пользователями дополнительного (OOB, *аббр. от* Out-Of-Band) канала: визуального, акустического, вибрационного, тактильного или магнитометрического [5–14]. Дополнительный канал образуется между двумя мобильными устройствами при личной встрече пользователей, при этом не требуется передача какой-либо информации по каналу связи, что затрудняет проведение атак со стороны злоумышленника. Будем для краткости называть обмен данными по дополнительному каналу с целью выработки идентичных последовательностей *сопряжением мобильных устройств*.

Поскольку участие пользователей при сопряжении неизбежно, решающими факторами в выборе способа сопряжения являются удобство использования и безопасность передаваемых данных. Кроме того, поскольку канал OOB обладает низкой пропускной способностью, объем информации, передаваемой по нему, должен быть сведен к минимуму.

Сравнительная характеристика дополнительных каналов приведена в работах [5, 14]. Любой из рассмотренных каналов может быть применен для выработки двоичных последовательностей с целью их последующего использования для аутентификации *DH*-значений. В явном виде последовательности вырабатываются при применении акселерометров или магнитометров. Поэтому эти способы в наибольшей степени подходят для решения исследуемой в работе задачи. Рассмотрим их более подробно.

Вибрационный канал. Использование вибрационного канала представляется возможным для устройств, содержащих в себе датчики акселерометра. Два мобильных устройства, содержащие датчики акселерометра, необходимо встряхивать пользователем в одной руке в течение примерно 5 с [12]. В это время осуществляется считывание информации о положении мобильного устройства в пространстве и преобразование ее в цифровой код. Два устройства (A и B), которые трясли вместе, на выходе получат схожие последовательности.

Магнитометрический канал. Пользователям необходимо удерживать два устройства вблизи друг к другу несколько секунд без выполнения каких-либо дополнительных операций. Устройства считывают собственные показания датчиков магнитометра и обмениваются ими. Сопряжение мобильных устройств с использованием магнитометрического канала, по сравнению с вибрационным, обеспечивает более высокую скорость работы (4,5 с), низкую вероятность ошибочной аутентификации и позволяет минимизировать участие пользователя в процессе сопряжения устройств, что указывает на преимущество магнитометрического канала для выработки случайных последовательностей [5]. Поэтому далее мы будем предполагать, что используется этот канал, хотя в принципе возможно применение и других каналов.

Сценарий сопряжения мобильных устройств, формирования ключа с аутентификацией *DH*-значений включает четыре этапа (рисунок 1).

Этап 1. Алиса и Боб проводят процедуру сопряжения мобильных устройств (смартфонов). Для этого они располагают устройства достаточно близко друг к другу (касаются друг друга) и удерживают несколько секунд. В это время в каждом смартфоне производится измерение магнитного поля Земли по трем пространственным осям. Значения магнитного поля квантуются, и из них формируются двоичные последовательности.

В процессе измерений поля между устройствами осуществляется локальный обмен данными, например, по каналу Bluetooth, для коррекции измерительных базисов устройств с целью обеспечения их идентичности. В итоге каждое устройство формирует случайную двоичную последовательность необходимой длины. Эти последовательности пользователи записывают в память своих устройств и будут использовать по мере необходимости как ключи в процедуре аутентификации *DH*-значений по каналу связи. Обозначим сформированные пользователями *A* и *B* последовательности, как ***a*** и ***b***, соответственно.

В [5] подробно описан процесс сбора и коррекции данных магнитометров. Мы не будем приводить эти результаты, поскольку они составляют предмет отдельного исследования, отметим лишь, что нами были проведены аналогичные исследования [15], которые подтвердили результаты работы [5]. Вероятность совпадения бит двух последовательностей от разных устройств в наших экспериментах составила 0,94.

Предполагается, что нарушитель также имеет магнитометр и на этапе сопряжения может быть расположен достаточно близко к сопрягаемым устройствам, но не в точке сопряжения, что определяется организационными ограничениями. Перехват данных коррекции нарушителем возможен, но это не приводит к утечке данных, полученных от магнитометров.

Этап 2. Этот и последующие этапы могут проводиться в любое другое время после процедуры сопряжения. Алиса и Боб вырабатывают секретные числа *x, y*, соответственно, вычисляют *DH*-значения и обмениваются ими, используя канал связи между ними. Канал связи может контролироваться нарушителем. Он может выполнять пассивные и активные атаки на передаваемую информацию.

Этап 3. С целью защиты от атак нарушителя проводится аутентификация переданных по каналу *DH*-значений на основе полученных на первом этапе последовательностей ***a*** и ***b***, с использованием аутентификаторов, формируемых согласно алгоритму Вегмана – Картера.

Этап 4. Если аутентификация *DH*-значений в обе стороны прошла успешно, то Алиса и Боб, используя имеющиеся у них случайные числа *x, y*, соответственно, вычисляют ключи, по методу *DH*. Эти ключи можно считать также аутентифицированными, так как они получены из секретных чисел *x, y* и аутентифицированных *DH*-значений $Y_{аут}$ и $X_{аут}$. Ключи могут быть использованы для шифрования информации, передаваемой между пользователями.

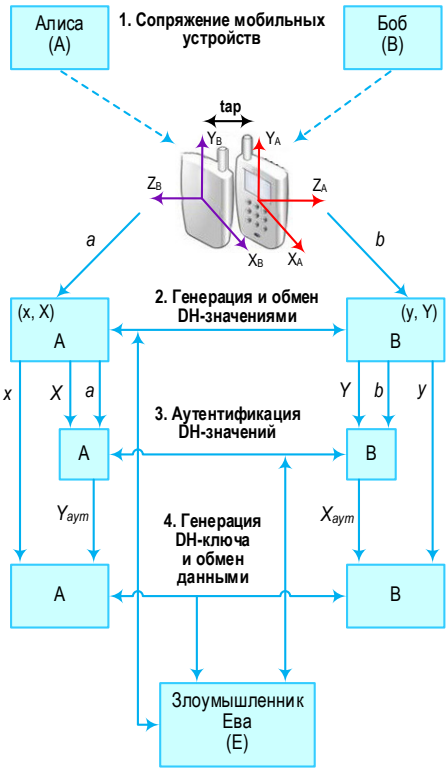

Рис. 1. Сценарий сопряжения мобильных устройств и формирования ключа Диффи – Хеллмана с аутентификацией

Fig. 1. Scenario for Pairing Mobile Devices and Generating a Diffie – Hellman Key with Authentication

В [5] предложен протокол Magpairing для создания корреспондентами *A* и *B* случайных последовательностей на основе магнитометрического канала и их использования для аутентификации *DH*-значений. Однако, как показано в [16], этот способ подвержен атаке «человек-посередине». В [16] также предложен способ устранения этой уязвимости на основе использования аутентифицирующих помехоустойчивых кодов [17, 18]. Показано, что для аутентификации *DH*-значений требуется длина аутентифицирующих последовательностей в несколько раз бóльшая, чем длины *DH*-значения. В [19, 20] исследован способ аутентификации *DH*-значений путем разделения *DH*-значения на блоки и формирования для каждого блока аутентификатора с помощью использования универсальных хэширующих функции, ключем для которых являются биты распределенных последовательностей. Однако данный способ не позволяет оптимизиро-

вать длину ключа аутентификации. В настоящей работе для аутентификации *DH*-значений предложен способ на основе использования аутентифицирующих последовательностей, полученных на этапе сопряжения, и метода аутентификации с одноразовым ключом Вегмана – Картера [21]. Задача исследования заключается в выводе соотношений, по которым может быть осуществлен выбор параметров способа и оценена его эффективность.

Способ аутентификации значений Диффи – Хеллмана на основе предварительно распределенных последовательностей и алгоритма одноразового ключа Вегмана – Картера

Пусть пользователи сети (Алиса и Боб) имеют предварительно распределенные двоичные последовательности $\boldsymbol{a}$ и $\boldsymbol{b}$, соответственно. Символы в последовательностях равновероятны и взаимно независимы. Однако последовательности в точности не совпадают друг с другом. Представим вероятность несовпадения бит в последовательностях $\boldsymbol{a}$ и $\boldsymbol{b}$ как $p_m = P(a_i \neq b_i)$, где $i = 1, 2, \ldots, L$ – номер символа в последовательностях.

Предполагаем, что злоумышленник Ева во время процедуры получения (выработки) аутентифицирующих последовательностей легальными пользователями удален от них, поэтому вероятность несовпадения бит в последовательностях у злоумышленника и легального пользователя равна $p_e = P(a_i \neq e_i) = 1/2$, $i = 1, 2, \ldots, L$. Другими словами, нарушитель не имеет информации о распределенных между A и B аутентифицирующих последовательностях.

Для защиты от атаки «человек-посередине» Алиса и Боб используют следующую схему аутентификации. Алиса разделяет *DH*-значение X длиной n_0, бит на N блоков длиной m бит. Для каждого блока $\boldsymbol{u_i}$ вычисляется аутентификатор $\boldsymbol{w_i}$ длиной v бит на основе использования предварительно распределенной последовательности $\boldsymbol{a}$. Для аутентификации каждого следующего блока значения *DH* выбираются новые блоки в последовательности $\boldsymbol{a}$.

Боб проводит аутентификацию значения *DH* следующим образом. Для каждого принятого блока $\boldsymbol{u_i}$ вычисляется аутентификатор $\boldsymbol{w_i'}$ (при этом используется имеющаяся у Боба последовательность $\boldsymbol{b}$), который сравнивается с аутентификатором $\boldsymbol{w_i}$, полученным по каналу связи. Если $\boldsymbol{w_i = w_i'}$, то блок $\boldsymbol{u_i}$ аутентифицирован. Если $w_i \neq w_i'$, то блок $\boldsymbol{u_i}$ не аутентифицирован.

DH-значение считается аутентифицированным в целом, если среди N принятых блоков окажутся не аутентифицированными не более Δ блоков ($1 \leq \Delta \leq N$). После этого аналогичным порядком проводится аутентификация *DH*-значения передаваемого от Боба к Алисе.

В [21] формирование аутентификаторов осуществлялось по алгоритму Вегмана – Картера (WCA, *аббр. от* Wegman-Carter Algorithm) с использованием универсальных хэш-функций [22]. Суть этого алгоритма следующая.

Представим каждый блок $\boldsymbol{u_i}$, как элемент поля Галуа $GF(2^m)$.

Аутентификатор w_i длиной v бит для блока u_i вычисляется по выражению $w_i = [u_i \times k_{1i} + k_{2i}]_v$, где $k_{1i}, k_{2i} \in GF(2^m)$, $i = 1, 2, \ldots, N$– ключ аутентификации [21]. Знаки $\times, +$ обозначают, соответственно, умножение и сложение в конечном поле $GF(2^m)$, а $\lfloor \cdot \rfloor_v$ – «усечение», то есть выбор v левых или правых элементов последовательности в квадратных скобках. Ключи $k_{1i}, k_{2i} \in GF(2^m)$ длиной m бит выбираются поочередно из последовательности $\boldsymbol{a(b)}$. Для каждого очередного блока $\boldsymbol{u}$ формируется новый аутентификатор $\boldsymbol{w}$ с использованием новой пары ключей $k_{1i}, k_{2i} \in GF(2^m)$. Вероятность навязывания ложного блока при известных $\boldsymbol{u}$ и $\boldsymbol{w}$ для данного способа аутентификации определяется соотношением $P_s = 1/2^v$ [21].

Общий расход ключа для аутентификации всего сообщения равен $L = 2mN = n_0$, и не зависит от длины аутентификатора, что является недостатком этого способа.

В настоящей работе предлагается для аутентификации *DH*-значения использовать метод Вегмана – Картера с одноразовым ключем (WCA OTP) [21]. Суть алгоритма состоит в том, что аутентификатор для каждого блока *DH*-значения вычисляется на одном ключе, после чего аутентификаторы блоков шифруются одноразовым ключом.

То есть аутентификатор w_i для блока $\boldsymbol{u_i}$ вычисляется следующим образом:

$$w_i = (u_i \times k_1 + k_2)_v + k'_i, \qquad (1)$$

где $k_1, k_2 \in GF(2^m)$ – основной ключ аутентификации длиной $2m$ бит, постоянный при аутентификации всего сообщения (*DH*-значения); $k'_i \in GF(2^m)$, $i = 1, 2, \ldots, N$ дополнительный ключ – индивидуальный для каждого блока $\boldsymbol{u_i}$ длиной v бит; ключи k_1, k_2, k'_i выбираются как непересекающиеся блоки в последовательности $\boldsymbol{a}$.

Из (1) следует, что длина ключа аутентификации (минимальная длина последовательности $\boldsymbol{a}$, необходимая для аутентификации значения *DH*) вычисляется как $L = 2m + vN$.

Будем считать, что нарушитель (Ева) имеет возможность создания атаки «человек-посередине», заключающейся в перехвате *DH*-значения одного корреспондента (A) и его обработке и пересылке другому корреспонденту (B) под видом A, преследуя цель стать посредником между A и B. Эта атака имеет три варианта исполнения.

Атака *имперсонализации.* Ложное *DH*-значение $X' = g^{x'}$ создается нарушителем без предварительно-

ного приема истинного *DH*-значения от корреспондента *A*. Далее генерируются аутентификаторы к каждому блоку X'. Сообщение и аутентификаторы передается корреспонденту *B*. Корреспондент *B* выполняет процедуру аутентификации.

Атака *отражения.* Нарушитель перехватывает *DH*-значение $X = g^x$ длиной n_0 бит, передаваемое в виде блоков u_i и аутентификаторов w_i, $i = 1, 2, \ldots, N$, и возвращает его корреспонденту *A*, корреспондент *A* проводит процедуру аутентификации.

Атака *подмены.* Нарушитель перехватывает *DH*-значение $X = g^x$ длиной n_0 бит, передаваемое в виде блоков u_i и аутентификаторов w_i, $i = 1, 2, \ldots, N$, генерирует ложное сообщение $X' = g^{x'}$, отличающееся от исходного в *D* блоках, и формирует аутентификаторы к нему по следующему правилу:

– если блоки u_i в исходном и ложном сообщении совпали, он использует перехваченные аутентификаторы;

– если блоки не совпали, нарушитель формирует аутентификаторы случайным образом.

DH-значение *X'* и аутентификаторы к нему нарушитель передает корреспонденту *B*, выдавая себя за корреспондента *A*. Корреспондент *B* выполняет процедуру аутентификации.

Параметры и оценка эффективности способа аутентификации

Оценку эффективности аутентификации *DH*-значения будем осуществлять по следующим параметрам:

P_f – вероятность ложного отклонения *DH*-значения легальным пользователем в отсутствие навязывания (событие наступает, когда число неправильно аутентифицированных блоков равно Δ и более из-за несогласованности аутентифицирующих последовательностей ***a*** и ***b***);

P_i – вероятность имперсонализации (событие наступает при проведении нарушителем атаки имперсонализации, когда ложное *DH*-значение создается без предварительного приема истинного *DH*-значения и принимается как истинное);

P_{ref} – вероятность успеха атаки отражения (событие наступает, когда нарушитель возвращает принятое от Алисы (или Боба) *DH*-значение ему обратно, а корреспондент принимает его как сообщение от противоположного корреспондента);

P_s – вероятность подмены *DH*-значения (событие наступает, когда нарушитель перехватывает истинное *DH*-значение, анализирует его и создает ложное *DH*-значение, которое принимается легальным пользователем, как истинное);

P_d – вероятность навязывания ложного *DH*-значения: $P_d = \max(P_i, P_{ref}, P_s)$;

L – длина ключа аутентификации (длина последовательностей ***a*** и ***b***), необходимая для аутентификации *DH*-значения длиной n_0 с заданными значениями P_f, P_d;

$W = vN$ – суммарная длина аутентификаторов *DH*-значения.

Задачу оптимизации системы аутентификации сформулируем как задачу выбора параметров m и v, при которых минимизируется длина ключа, необходимая для аутентификации *DH*-значения длиной n_0 бит при выполнении неравенств: $P_f \le \tilde{P}_f$, $P_d \le \tilde{P}_d$, где $\tilde{P}_f$, $\tilde{P}_d$ – заданные требования по вероятности ложной аутентификации и вероятности навязывания.

Найдем оценки этих параметров.

Заметим, что основной ключ участвует в формировании аутентификатора каждого блока, поэтому если биты этого ключа, выбираемые из аутентифицирующих последовательностей пользователей, у корреспондентов не совпадают (есть ошибка в основном ключе), то все аутентификаторы на приеме будут оцениваться, как случайные. С другой стороны, индивидуальные ключи влияют только на аутентификаторы блоков длиной v бит.

Поэтому формула для вероятности ложного отклонения *DH*-значения имеет вид:

$$P_f(\Delta) = P_b(k_1, k_2) \sum_{i=\Delta+1}^{N} C_N^i \left(\frac{1}{2^v}\right)^{N-i} \left(1 - \frac{1}{2^v}\right)^i + \\ + \left(1 - P_b(k_1, k_2)\right) P_f{}'(\Delta), \qquad (2)$$

где первое слагаемое есть вероятность ложного отклонения *DH*-значения, когда основной ключ содержит ошибки с вероятностью $P_b(k_1, k_2)$ и, как следствие, аутентификаторы формируются как случайные блоки длиной v бит. Второе слагаемое есть вероятность ложного отклонения *DH*-значения, когда основной ключ не содержит ошибки вероятностью $(1 - P_b(k_1, k_2))$, а P'_f есть вероятность суммы событий, состоящих в том, что в принятой последовательности X из-за ошибок в аутентифицирующих последовательностях окажутся не аутентифицированными Δ+1 и более блоков. P'_f может быть найдена как:

$$P'_f(\Delta) = \sum_{i=\Delta+1}^{N} C_N^i p_v^i (1 - p_v)^{N-i}, \qquad (3)$$

где p_v – вероятность несовпадения ключей k'_i, то есть вероятность несовпадения блоков длиной v бит, выбранных их последовательностей ***a*** и ***b*** и равна $p_v = 1 - (1 - p_m)^v$ в предположении, что ошибки в битах распределены по закону Бернулли.

Вероятность успешной атаки имперсонализации можно получить, как оценку количества обнаруженных и необнаруженных ложных аутентификаторов в *N* блоках, при их случайном генерировании.

Вероятность успешного навязывания ложного аутентификатора длиной v символов равна вероятности угадывания ключа k'_i в (1) и равна $\frac{1}{2^v}$:

$$P_i(\Delta) = \sum_{i=0}^{\Delta} C_N^i (\frac{1}{2^v})^{(N-i)} (1 - \frac{1}{2^v})^i. \quad (4)$$

Вероятность атаки отражения P_{ref} определим из следующих соображений. Согласно описанному алгоритму, аутентификаторы для каждого блока создаются на основе индивидуальных ключей, выбираемых как подблоки последовательностей ***a*** и ***b***. Поэтому принимаемое от Евы под видом Боба *DH*-значение Алиса будет аутентифицировать на основе номеров блоков, которые должен был бы использовать Боб, но не номеров блоков ключа, которые использовала Алиса при создании аутентификаторов для своего *DH*-значения. Эти блоки ключей аутентификации, очевидно, не совпадут, что равносильно аутентификации *DH*-значения на случайных ключах, следовательно $P_{\text{ref}} = P_i$.

Для оценки вероятности подмены рассмотрим стратегию нарушителя, из п. 2. Подмену нарушителем истинного *DH*-значения ложным значением можно рассматривать как последовательное наступление двух событий: создание нарушителем ложного *DH*-значения, отличающегося от истинного в D блоках размерности m. (обозначим вероятность этого события – $P_g(D)$) и события, состоящего в навязывании этого сообщения путем формировании аутентификаторов для блоков, отличающихся в ложном *DH*-значении от блоков истинного *DH*-значения. В ходе подмены ложное *DH*-значение принимается легальным пользователем как истинное; вероятность навязывания такого *DH*-значения – $P_r(D)$.

Таким образом вероятность подмены равна:

$$P_s(D) = P_g(D) P_r(D). \quad (5)$$

Рассмотрим оба сомножителя. Очевидно, что чем меньше отличаются X и X', тем легче нарушителю реализовать атаку «человек–посередине». Заметим, что непосредственно значение X' нарушитель выбрать не может. Сначала он выбирает x', затем находит значение экспоненты $X' = g^{x'} \bmod p$. Если x' выбирать случайно из множества чисел от 0 до $p - 1$, то число X' будет также случайным числом из множества чисел от 0 до $p - 1$. При большой величине модуля p ($p \approx 2^{256}$) нахождение отображения $x' \Leftrightarrow X'$ требует необозримо больших вычислительных затрат. Поэтому разумной стратегией для нарушителя будет случайный выбор числа x', что равносильно случайному выбору X'.

Вероятность случайного формирования нарушителем ложного *DH*-значения X', отличающегося от перехваченного значения X в D блоках, может на основе комбинаторных рассуждений о выпадений одинаковых значений двух 2^m-гранных игральных костей, при N бросаниях записана как:

$$P_g(D) = C_N^D \left(\frac{1}{2^m}\right)^{N-D} \left(1 - \frac{1}{2^m}\right)^D. \quad (6)$$

Вероятность навязывания сформированного ложного *DH*-значения, отличающегося от истинного значения в D блоках в зависимости от порога принятия решения Δ, можно оценить:

$$P'_r(\Delta, D) \le \sum_{i=0}^{\Delta} C_D^i (\frac{1}{2^v})^{(D-i)} (1 - \frac{1}{2^v})^i \times \times \sum_{j=0}^{t} C_{(N-D)}^j p_b^j (1 - p_b)^{(N-D-j)}, \quad (7)$$

где $t = \begin{cases} N - D, & \text{если } \Delta - i \ge N - D. \\ \Delta - i, & \text{если } \Delta - i < N - D \end{cases}$.

Первая сумма в (7) характеризует вероятность фиксации на приеме i ложных аутентификаторов ($0 \le i \le \Delta$), которые обнаруживаются и D-i ложных аутентификаторов, которые не обнаруживаются. Вторая сумма – вероятность несовпадения j ($0 \le \le j \le t$) из N-D аутентификаторов исходного сообщения, которые нарушителем были переданы без изменений (несовпадение произошло за счет несовпадения ключей в аутентифицирующих последовательностях ***a*** и ***b***). Неравенство в (7) объясняется тем, что при проверке D аутентификаторов, которые были сформированы нарушителем случайным образом, ошибки в аутентифицирующих последовательностях не учитывались (для точного расчета нужно оценить вероятность того, что определенная конфигурация ошибки в аутентифицирующих ключах, приведет к тому, что ложный аутентификатор будет принят как правильный, но вероятность этого события мала).

Так же как и при выводе формул для вероятности ложной аутентификации, необходимо учесть случаи правильного и ошибочного приема основного ключа легальными пользователями из последовательностей ***a*** и ***b***. Если основной ключ содержит ошибку, то все аутентификаторы будут восприниматься как ложные. Если основной ключ без ошибок, то аутентификаторы, верифицируемые как ложные, определяются только ошибками в ключах аутентификации и ошибками в аутентификаторах, выбранных злоумышленником случайным образом. Суммарное количество аутентификаторов не должно превышать порог Δ.

Таким образом, формулу вероятности подмены можно записать в виде:

$$P_r(\Delta, D) = P_b(k_1, k_2) \sum_{i=0}^{\Delta} C_N^i (\frac{1}{2^v})^{N-i} \left(1 - \frac{1}{2^v}\right)^i + + \left(1 - P_b(k_1, k_2)\right) P'_r(\Delta, D), \quad (7)$$

где $P'_r(\Delta)$ – вероятность подмены N блоков длиной v бит рассчитывается по формуле (7).

Нарушитель может применить любую стратегию создания ложного *DH*-значения (может использовать любое D), поэтому определим вероятность подмены (при фиксированном значении Δ) следующим образом:

$$P'_s = \max_D P_g(D)P_r(D). \quad (9)$$

Из соотношений (2), (8) следует, что вероятности ложного отклонения и подмены критично зависят от вероятности ошибки основного ключа $P_b(k_1, k_2)$, где k_1, k_2 – это блок из $2m$ символов. Этот ключ является одинаковым при формировании аутентификаторов для всех блоков, поэтому рассмотрим пути повышения достоверности формирования этого ключа длиной $2m$ бит. С этой целью может быть применено помехоустойчивое кодирование с шифрованием. Рассмотрим простой способ, основанный на использовании кода повторения [23].

Пользователь A генерирует случайный бит $z = (0,1)$, повторяет его s раз, то есть применяет помехоустойчивый $(s,1)$-код повторения. Кодовое слово $\bar{z}$ суммирует по модулю два с блоком последовательности $\bar{a}$ длиной s бит, получает блок $\bar{y} = \bar{z} \oplus \bar{a}$ и передает его по служебному каналу пользователю B. Пользователь B суммирует принятый от A блок $\bar{y}$ со своим блоком последовательности $\bar{b}$, получает $\bar{y} \oplus \bar{b} = \bar{z} \oplus \bar{a} \oplus \bar{b}$. В принимает решение о приеме бита z', если все s бит в блоке $\bar{y} \oplus \bar{b}$ одинаковые. Если биты разные, этот блок стирается. По обратному служебному каналу он сообщает о своем решении A. Если B стер блок, то A тоже его стирает.

Ошибочный прием блока из s повторений бита имеет место тогда, когда все биты в блоке приняты в инверсном виде, тогда вероятность ошибки бита z:

$$\tilde{p}_m = \frac{p_m^s}{(1-p_m)^s + p_m^s},$$

а вероятность ошибки в основном ключе:

$$P_b(k_1, k_2) = 1 - (1 - \tilde{p}_m)^{2m}. \quad (10)$$

Нарушитель наблюдает за сообщениями в служебном канале и удаляет блоки, если их удалили легальные корреспонденты. С оставленными блоками он проводит такую же процедуру обработки, что и корреспондент B. По условию вероятность ошибки в аутентифицирующей последовательности нарушителя относительно пользователя A равна $p_e = 1/2$. Поэтому декодирование $(s,1)$-кода равносильно их угадыванию бита z.

В среднем, для формирования одного бита с повышенной достоверностью необходимо при использовании данного способа затратить $t = \frac{s}{(1-p_m)^s + p_m^s}$ бит аутентифицирующих последовательностей. При использовании данного способа повышения достоверности основного ключа можно найти длину аутентифицирущей последовательности, необходимой для аутентификации DH-значения в целом.

Длина ключа аутентификации может быть найдена как сумма количества бит необходимых для формирования основного ключа с заданной достоверностью и количества бит, необходимых для формирования аутентификаторов для всех блоков:

$$L(m, v, s) = \frac{2ms}{p_m^s + (1 - p_m^s)} + \frac{n_0 v}{m}. \quad (11)$$

Оптимальным набором параметров (m, v, s) будем считать такой набор, при котором:

$$L(m, v, s) \to L_0,$$

где $L_0 = \min_{m,v,s} L(m, v, s)$ при условии $P_{f2} \le \tilde{P}_f, P_d \le \tilde{P}_d$.

Заметим, что суммарная длина аутентификаторов W определяет затраты данного способа аутентификации с точки зрения времени использования канала связи между пользователями, необходимого для передачи аутентификаторов. Несложно увидеть, что $W = L(m, v, s)$, поэтому оптимизация параметра L оптимизирует и параметр W.

Пример оценки параметров системы аутентификации

Предположим, что проводится аутентификация DH-значения длиной $n_0 = 256$ бит, что является стандартной длиной во многих шифрах [24, 25]. Вероятность отличия бит в аутентифицирующих последовательностях $p_m = 0{,}05$.

К системе аутентификации предъявлены следующие требования:

– вероятность ложного отклонения DH-значения $P_f \le \tilde{P}_f$;

– вероятность навязывания $P_d \le \tilde{P}_d$ и $\tilde{P}_f = \tilde{P}_d = 10^{-6}$.

На рисунке 2 показаны зависимости вероятности ложного отклонения DH-значения P_f от порога Δ для длин блоков m = 1, 2, 4, 8 и длин аутентификаторов v, равных длине блока (сплошные линии), рассчитанных согласно (2). Также здесь показаны зависимости P_f для длин v аутентификаторов меньших, чем длины блока. Вероятности ошибки в основном ключе $P_b(k_1, k_2)$ рассчитаны для кодов повторения $(s,1)$ при $s = 4$ и $s = 6$. Из рисунка 2 видно, что зависимости P_f от Δ имеют три явно выраженных участка. Верхняя часть каждой зависимости определяется вторым членом в (2), средняя часть определяется первым множителем первого слагаемого и соответствует вероятности ошибки основного ключа $P_b(k_1, k_2)$. Нижняя часть определяется вторым множителем первого слагаемого. Видим, что выбирая число повторений $(s,1)$-кода, можно получить значение $P_f \le \tilde{P}_f$. Следует отметить, что P_f зависит от длины аутентификатора v, причем при уменьшении v P_f также уменьшается (штриховые линии).

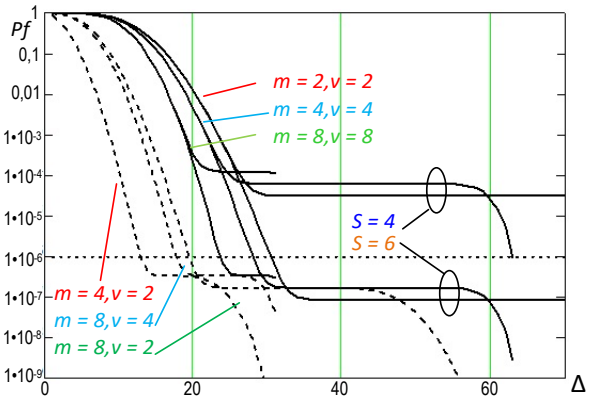

Рис. 2. Зависимость вероятности ложного отклонения *DH*-значения от порога Δ при разных длинах аутентифицируемых блоков *m*, разных длинах аутентификаторов *v* для двух значений длины кода повторения *s*

Fig. 2. Dependence of the Probability of False Alarm of the DH-Value from the Threshold Δ for Different Lengths of Authenticated Blocks m, Different Lengths of Authenticators v for Two Values of the Repetition Code Length s

Обозначим $\Delta_{\min} = \min\Delta$, при котором $P_f \le \tilde{P}_f$ для фиксированных значений (m, v). Значения $\Delta_{\min}$ для различных пар (m, v) приведены в таблице 1.

ТАБЛИЦА 1. Минимальные значения порога $\Delta_{\min}$ для разных *m, v*

TABLE 1. The Minimum Threshold Values Δ_{min} for Different m, v

m \ v	1	2	3	4	6	8
1	33					
2	21	31				
4	14	20	25	29		
8		13	16	18	22	24

Для этих значений $\Delta_{\min}$ построены зависимости вероятности подмены $P_s(D) = P_g(D) \cdot \mathrm{P_r}(D)$, согласно (9) от количества блоков D, в которых могут отличаться истинное и ложное *DH*-значения для разных значений аутентифицируемых блоков и разных значений длин аутентификаторов этих блоков (рисунок 3).

Видим, что для всех представленных (см. рисунок 3) значений параметров (m, v) выполняется условие $P'_s \le \tilde{P}_d = 10^{-6}$ для любых значений D. В этом случае попытка нарушителя подобрать ложное сообщение, отличающееся от истинного *DH*-значения в малом количестве блоков и навязать его получателю будет безуспешной.

В таблице 2 представлены значения P_f, P_s, для выбранных параметров m, v, $\Delta_{\min}$, удовлетворяющие условиям $P_f \le \tilde{P}_f = 10^{-6}$, $P_s \le \tilde{P}_d = 10^{-6}$. Также здесь приведены вероятности имперсонализации P_i, согласно соотношению (4). Анализ таблицы показывает, что для двух сочетаний параметров (m, v): (4, 1) и (8, 2) $P_i > \tilde{P}_d$, поэтому эти параметры не удовлетворяют заданным требованиям.

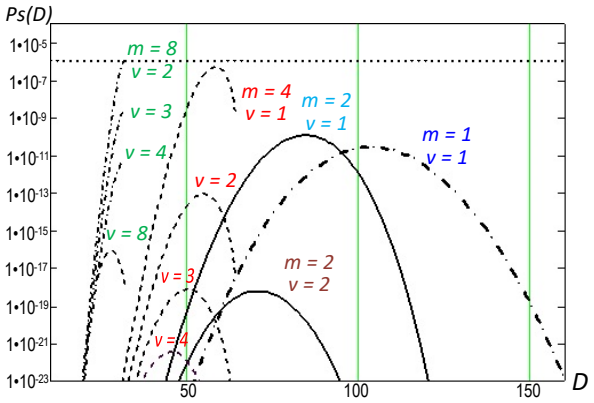

Рис. 3. Зависимость вероятности подмены от параметра *D* при разных длинах аутентифицируемых блоков *m*, разных длинах аутентификаторов *v* при выполнении условия $\Delta = \Delta_{\min}$ и *s* = 6

Fig. 3. Dependence of the Substitution Probability on the Parameter D for Different Lengths of Authenticated Blocks m, Different Lengths of Authenticators v when the Condition is $\Delta = \Delta_{\min}$ and s = 6

ТАБЛИЦА 2. Вероятности ложного обнаружения P_f, имперсонализации P_i, подмены P_s и навязывания P_d для разных значения *m* и v при аутентификации *DH*-значения длиной 256 бит

TABLE 2. The Probabilities of false Detection P_f, Impersonalization P_i, Substitution P_s and Imposition P_d for Different Values of m and v When Authenticating a 256-bit DH-Value

(m, v)	$P_f \le \tilde{P}_f$	$P_s \le \tilde{P}_d$	P_i	$P_d = \max(P_s, P_i)$
(1, 1)	$3{,}0 \cdot 10^{-7}$	$2{,}7 \cdot 10^{-11}$	$4{,}0 \cdot 10^{-36}$	$2{,}7 \cdot 10^{-11}$
(2, 2)	$5{,}8 \cdot 10^{-7}$	$5{,}5 \cdot 10^{-19}$	$3{,}0 \cdot 10^{-33}$	$5{,}5 \cdot 10^{-19}$
(2, 1)	$4{,}9 \cdot 10^{-7}$	$1{,}1 \cdot 10^{-10}$	$2{,}2 \cdot 10^{-15}$	$1{,}1 \cdot 10^{-10}$
(4, 4)	$4{,}0 \cdot 10^{-7}$	$3{,}5 \cdot 10^{-22}$	$1{,}6 \cdot 10^{-25}$	$3{,}5 \cdot 10^{-22}$
(4, 3)	$4{,}0 \cdot 10^{-7}$	$7{,}0 \cdot 10^{-19}$	$9{,}4 \cdot 10^{-20}$	$7{,}0 \cdot 10^{-19}$
(4, 2)	$5{,}4 \cdot 10^{-7}$	$8{,}9 \cdot 10^{-14}$	$2{,}4 \cdot 10^{-13}$	$8{,}9 \cdot 10^{-14}$
(4, 1)	$6{,}4 \cdot 10^{-7}$	$5{,}2 \cdot 10^{-7}$	$3{,}5 \cdot 10^{-6}$	$3{,}5 \cdot 10^{-6}$
(8, 8)	$6{,}7 \cdot 10^{-7}$	$8{,}8 \cdot 10^{-17}$	$5{,}2 \cdot 10^{-13}$	$8{,}8 \cdot 10^{-17}$
(8, 6)	$4{,}5 \cdot 10^{-7}$	$6{,}7 \cdot 10^{-15}$	$4{,}1 \cdot 10^{-11}$	$6{,}7 \cdot 10^{-15}$
(8, 4)	$6{,}9 \cdot 10^{-7}$	$4{,}0 \cdot 10^{-12}$	$2{,}2 \cdot 10^{-9}$	$4{,}0 \cdot 10^{-12}$
(8, 3)	$6{,}1 \cdot 10^{-7}$	$1{,}9 \cdot 10^{-9}$	$2{,}9 \cdot 10^{-7}$	$1{,}9 \cdot 10^{-9}$
(8, 2)	$9{,}4 \cdot 10^{-7}$	$6{,}7 \cdot 10^{-7}$	$3{,}8 \cdot 10^{-5}$	$3{,}8 \cdot 10^{-5}$

Тем не менее, есть достаточно вариантов выбора параметров (m, v), удовлетворяющих требованиям $P_f \le \tilde{P}_f = 10^{-6}$, $P_s \le \tilde{P}_d = 10^{-6}$ и поэтому окончательный выбор этих параметров будет определяться задачей оптимизации суммарной длины ключа аутентификации L и суммарной длиной всех аутентификаторов W.

В таблице 3 приведены значения $L(m, v, s)$ для разных значений параметров (m, v) при s = 6 и выполнении требований: $\tilde{P}_f = 10^{-6}, \tilde{P}_d = 10^{-6}$, рассчитанные согласно (11).

Очевидно, что наименьшее значение $L_0 = 130$ имеет место при m = 4, v = 1. Однако согласно таблице 2 для этих параметров не выполняется

требование по вероятности имперсонализации $P_i = 3{,}5 \cdot 10^{-6} > 10^{-6}$. Поэтому следует выбрать следующее минимальное значение $L_0 = 194$ при $m = 4$, $v = 2$.

ТАБЛИЦА 3. Расход ключа аутентификации

TABLE 3. Authentication Key Consumption

m \ v	1	2	3	4	6	8
1	272					
2	167	287				
4	130	194	258	322		
8		195	227	259	323	387

Таким образом, аутентификация *DH*-значения длиной 256 бит с выполнением требований $\tilde{P}_f = 10^{-6}, \tilde{P}_d = 10^{-6}$ при допустимой вероятности несовпадения бит в аутентифицирующих последовательностях $p_m = 0{,}05$ может быть обеспечена при длине $\tilde{P}_f = 10^{-6}$, $\tilde{P}_d = 10^{-6}$е блока аутентификации $m = 4$, длине аутентификатора блока $v = 2$. Для аутентификации *DH*-значения необходимо использовать в среднем 194 бита аутентифицирующих последовательностей. Полученный результат можно сравнить с результатами работ [16] и [21]. При тех же требованиях $\tilde{P}_f = 10^{-6}$, $\tilde{P}_d = 10^{-6}$для аутентификации *DH*-значения длиной 256 бит при использовании метода на основе помехоустойчивых кодов [16] требуется 768 бит ключа при допустимой вероятности несовпадения бит в аутентифицирующих последовательностях $p_m = 0{,}01$ (при $p_m = 0{,}05$ аутентификация с заданными требованиями невозможна). При использовании способа аутентификации на основе универсальных хеш-функций [21] длина ключа равна 512 бит. То есть предложенный способ аутентификации *DH*-значений имеет преимущество перед другими способами по расходу ключа аутентификации.

Заключение

В работе исследуются способ аутентификации DH-значений (g^x), формируемых при генерации сеансового ключа по методу Диффи – Хеллмана между двумя мобильными устройствами, имеющими предварительно распределенные между ними двоичные случайные цепочки бит. Эти последовательности пользователи вырабатывают в ходе процедуры сопряжения своих мобильных устройств во время личной встречи. Показано, что для этого могут быть использованы акселерометры или магнитометры, входящие в состав современных мобильных устройств. Использование магнитометрического канала, по сравнению с вибрационным, обеспечивает более высокую скорость работы, низкую вероятность ошибочной аутентификации и позволяет минимизировать участие пользователя в процессе сопряжения устройств, что указывает на преимущество магнитометрического канала для выработки случайных последовательностей. Нарушитель в ходе процедуры сопряжения удален от пользователей и не получает доступа к сообщениям, которыми они обмениваются. Для аутентификации *DH*-значения предложен способ, состоящий в разбиении *DH*-значения, на N блоков длиной m бит и аутентификации блоков на основе метода одноразового ключа Вегмана – Картера, в роли которого выступают предварительно распределенные между корреспондентами цепочки случайных бит, которые могут не совпадать в точности между собой. Если число не аутентифицированных блоков меньше порога Δ, аутентификация *DH*-значения считается пройденной. Выведены соотношения для оценки P_f – вероятности ложного отклонения *DH*-значения в отсутствие навязывания, P_i – вероятности имперсонализации, P_{ref} – вероятности успеха атаки отражения, P_s – вероятности подмены *DH*-значе-ния и P_d – вероятности навязывания ложного *DH*-значения, как максимума $(P_i, P_{\text{ref}}, P_s)$;

При выводе соотношения для нахождения P_d предложен подход, учитывающий возможности нарушителя не только по подмене истинного *DH*-значения ложным, но и возможности по созданию ложного *DH*-значения с заданным отличием в количестве блоков от истинного. Также для повышения достоверности первой части ключа аутентификации, выделяемой из распределенных последовательностей, предложено использование способа случайной передачи бит и использования кода повторения.

Таким образом, поставлена и решена задача оптимизации параметров (длина блока и собственно аутентификатора) с точки зрения минимизации расхода аутентифицирующей последовательности и суммарной длины всех аутентификаторов. Приведен пример выбора параметров для аутентификации *DH*-значения длиной 256 бит. Показано, что путем выбора параметров системы аутентификации, можно обеспечить достаточно малые значения вероятности ложной аутентификации и вероятности навязывания ложного ключа нарушителем $\tilde{P}_f = 10^{-6}$, $\tilde{P}_d = 10^{-6}$.

Список используемых источников

1. Diffie M., Hellman M. New directions in cryptography // IEEE Transactions on Information Theory. 1976. Vol. 22. Iss. 6. PP. 644–654. DOI:10.1109/TIT.1976.1055638

2. Mirzadeh S., Cruickshank H., Tafazolli R. Secure Device Pairing: A Survey // IEEE Communications Surveys & Tutorials. 2014. Vol. 16. PP. 17–40. DOI:10.1109/SURV.2013.111413.00196

3. Zeng K. Physical layer key generation in wireless networks: challenges and opportunities // IEEE Communications Magazin. 2015. Vol. 53. Iss. 4. PP. 20–27. DOI:10.1109/MCOM.2015.7120014

4. Zhang J., Duong T.Q., Marshall A., Woods R. Key Generation from Wireless Channels: a Review // IEEE Access. 2016. Vol. 4. PP. 614–626. DOI:10.1109/ACCESS.2016.2521718

5. Jin R., Shi L., Zeng K., Pande A., Mohapatra P. MagPairing: Pairing Smartphones in Close Proximity Using Magnetometer // IEEE Transactions on Information Forensics and Security. 2016. Iss. 6. PP. 1304–1319. DOI:10.1109/TIFS.2015.2505626

6. Mc Cune J., Perring A., Reiter M. Seeing-is-believing: using camera phones for human-verifiable authentication // Proceedings of the Symposium on Security and Privacy (S&P'05, Oakland, USA, 8–11 May 2005). IEEE, 2005. PP. 110–124. DOI:10.1109/SP.2005.19

7. Saxena N., Ekberg J.-E., Kostiainen K., Asokan N. Secure Device Pairing Based on a Visual Channel // Proceedings of the Symposium on Security and Privacy (S&P'06, Berkeley/Oakland, USA, 21–24 May 2006). IEEE, 2006. PP. 57–68. DOI:10.1109/SP.2006.35

8. Prasad R., Saxena N. Efficient Device Pairing Using "Human-Comparable" Synchronized Audiovisual Patterns // Proceedings of the 6th International Conference on Applied Cryptography and Network Security (ACNS 2008, New York, USA, 3–6 June 2008). Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2008. Vol. 5037. PP. 328–345. DOI:10.1007/978-3-540-68914-0_20

9. Goodrich M.T., Sirivianos M., Solis J., Soriente C., Tsudik G., Uzun E. Using Audio in Secure Device Pairing // International Journal of Security and Networks. 2009. Vol. 4. Iss. 1. PP. 57–68. DOI:10.1504/IJSN.2009.023426

10. Goodrich M.T., Sirivianos M., Solis J., Tsudik G. Uzun E. Loud and Clear: Human-Verifiable Authentication Based on Audio. Distributed Computing Systems // Proceedings of the 26th International Conference on Distributed Computing Systems (ICDCS 2006, Lisboa, Portugal, 4–7 July 2006). IEEE, 2006. PP. 1–10. DOI:10.1109/ICDCS.2006.52

11. Soriente C., Tsudik G., Uzun E. HAPADEP: Human-Assisted Pure Audio Device Pairing // Proceedings of the 11th International Conference on Information Security (ISC 2008, Taipei, Taiwan, 15–18 September 2008). Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2008. Vol. 5222. PP. 385–400. DOI:10.1007/978-3-540-85886-7_27

12. Mayrhofer R. Gellersen H. Shake Well Before Use: Intuitive and Secure Pairing of Mobile Devices // IEEE Transactions on Mobile Computing. 2009. Vol. 8. Iss. 6. PP. 792–806. DOI:10.1109/TMC.2009.51

13. Soriente C., Tsudik G., Uzun E. BEDA: Button-Enabled Device Association // Proceedings of the 1st International Workshop on Security for Spontaneous Interaction (IWSSI). Linz: Institute of Networks and Security, 2007. PP. 443–449.

14. Kumar A., Saxena N., Tsudik G., Uzun E. Caveat emptor: A comparative study of secure device pairing methods // Proceedings of the International Conference on Pervasive Computing and Communications (Galveston, USA, 9–13 March 2009). IEEE, 2009. PP. 1–10. DOI:10.1109/PERCOM.2009.4912753

15. Корпусов В.Д., Ольховой О.О., Яковлев В.А. Исследование датчика случайных чисел на основе магнитометра // VII Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (Санкт-Петербург, Россия, 28 февраля–1 марта 2018). СПб: СПбГУТ, 2018. С. 488–494.

16. Яковлев В.А. Аутентификация ключей, распределяемых методом Диффи-Хеллмана, для мобильных устройств на основе аутентифицирующих помехоустойчивых кодов и магнитометрических данных // Труды СПИИРАН. 2019. Т. 18. № 3. С. 705–740. DOI:10.15622/sp.2019.18.3.705-740

17. Maurer U. Information-Theoretically Secure Secret-Key Agreement by not Authenticated Public Discussion // Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques (Konstanz, Germany, 11–15 May 1997). Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 1997. Vol. 1233. PP. 209–223. DOI:10.1007/3-540-69053-0_15

18. Korzhik V., Yakovlev V., Morales-Luna G., Chesnokov R. Perfomance Evaluation of Keyless Authentication Based on Noisy Channel // Proceedings of the 4th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (MMM-ACNS 2007, St. Petersburg, Russia, 13–15 September 2007). Communications in Computer and Information Science. Berlin, Heidelberg: Springer, 2007. Vol. 1. PP. 115–126. DOI:10.1007/978-3-540-73986-9_9

19. Яковлев В.А. Способ аутентификации значений Диффи-Хеллмана на основе предварительно распределенных случайных последовательностей и хэширующих функций // X Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (Санкт-Петербург, Россия, 24–25 февраля 2021). СПб: СПбГУТ, 2021. С. 693–698.

20. Yakovlev V., Korzhik V., Adadurov S. Authentication of Diffie-Hellman Protocol for Mobile Units Executing a Secure Device Pairing Procedure in Advance // Proceedings of the 29th Conference of Open Innovations Association (FRUCT, Tampere, Finland, 12–14 May 2021). IEEE, 2021. DOI:10.23919/FRUCT52173.2021.9435495

21. Wegman M.N., Carter J.L. New Hash Functions and their Use in Authentication and Set Equality // Journal of Computer and System Sciences. 1981. Vol. 22. Iss. 3. PP. 265–279. DOI:10.1016/0022-0000(81)90033-7

22. Carter J.l., Wegman M.N. Universal classes of hash functions // Journal of Computer and System Sciences. 1979. Vol. 18. Iss. 2. PP. 143–154. DOI:10.1016/0022-0000(79)90044-8

23. Maurer U. Secret key agreement by public discussion from common information // IEEE Transactions on Information Theory. 1993. Vol. 39. Iss. 3. PP. 2535–2549. DOI:10.1109/18.256484

24. ГОСТ Р 34 12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015.

25. FIPS 197. Specification for the ADVANCED ENCRIPTION STANDARD (AES). Nov.2001.

* * *

Method for Authentication of Diffie – Hellman Values Based on Pre-Distributed Random Sequences and Wegman – Carter One-Time Pad Algorithm

V. Yakovlev[1]

[1]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Article info
DOI:10.31854/1813-324X-2021-7-3-79-90
Received 9th June 2021
Accepted 19th July 2021

For citation: Yakovlev V. Method for Authentication of Diffie – Hellman Values Based on Pre-Distributed Random Sequences and Wegman – Carter One-Time Pad Algorithm. *Proc. of Telecom. Universities.* 2021;7(3):79–90. (in Russ.) DOI:10.31854/1813-324X-2021-7-3-79-90

Abstract: *A method of authentication of keys generated by the Diffie-Hellman method is investigated in the context of the use of a man-in-the-middle attack by an attacker. It is assumed that the users Alice and Bob, who form the key, have pre-distributed random bit strings* ***a*** *and* ***b****, respectively, obtained either from some source or generated by themselves based on data obtained from magnetometers or accelerometers from mobile devices. The attacker has no access to these chains. A method for authenticating Diffie – Hellman values (DH values) is proposed. For this purpose, the message (DH-value) is divided by Alice into N blocks. For each block, an authenticator is calculated using the Wegman – Carter algorithm with a one-time pad keys, which are sequences* ***a*** *and* ***b.*** *The DH-value and authenticators are transmitted over the channel to Bob, who calculates authenticators from the received DH-value and compares them with the authenticators received from the channel. If the number of unauthenticated blocks does not exceed the set threshold, then DH-value authentication is considered successful. But the drawback of this method is a little disagreement between authenticating strings of different users. The formulas for probabilities of the undetected deception and the false alarm (due to the mismatch of chains* ***a*** *and* ***b****) are proved. The optimization of the method parameters (the number of blocks and the length of the authenticator) is carried out, at which the consumption of the authentication key (chains* ***a*** *and* ***b****) is minimized when the specified requirements for the probability of the undetected deception and the false alarm are met. Examples of the choice of authentication parameters for a 256-bit DH-value are given.*

Keywords: *Diffie – Hellman method, authentication, universal hash functions, Wegman – Carter one-time pad authentication.*

References

1. Diffie M., Hellman M. New directions in cryptography. *IEEE Transactions on Information Theory*. 1976;22(6):644–654. DOI:10.1109/TIT.1976.1055638
2. Mirzadeh S., Cruickshank H., Tafazolli R. Secure Device Pairing: A Survey. *IEEE Communications Surveys & Tutorials*. 2014;16:17–40. DOI:10.1109/SURV.2013.111413.00196
3. Zeng K. Physical layer key generation in wireless networks: challenges and opportunities. *IEEE Communications Magazine*. 2015;53(4):20–27. DOI:10.1109/MCOM.2015.7120014
4. Zhang J., Duong T.Q., Marshall A., Woods R. Key Generation from Wireless Channels: a Review. *IEEE Access*. 2016;4: 614–626. DOI:10.1109/ACCESS.2016.2521718
5. Jin R., Shi L., Zeng K., Pande A., Mohapatra P. MagPairing: Pairing Smartphones in Close Proximity Using Magnetometer. *IEEE Transactions on Information Forensics and Security*. 2016;6:1304–1319. DOI:10.1109/TIFS.2015.2505626
6. Mc Cune J., Perring A., Reiter M. Seeing-is-believing: using camera phones for human-verifiable authentication. *Proceedings of the Symposium on Security and Privacy, S&P'05, 8–11 May 2005, Oakland, USA*. IEEE; 2005. p.110–124. DOI:10.1109/SP.2005.19
7. Saxena N., Ekberg J.-E., Kostiainen K., Asokan N. Secure Device Pairing Based on a Visual Channel. *Proceedings of the Symposium on Security and Privacy, S&P'06, 21–24 May 2006, Berkeley/Oakland, USA*. IEEE; 2006. p.57–68. DOI:10.1109/SP.2006.35
8. Prasad R., Saxena N. Efficient Device Pairing Using "Human-Comparable" Synchronized Audiovisual Patterns. *Proceedings of the 6th International Conference on Applied Cryptography and Network Security, ACNS 2008, 3–6 June 2008, New York,*

USA. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer; 2008. vol.5037. p.328–345. DOI:10.1007/978-3-540-68914-0_20

9. Goodrich M.T., Sirivianos M., Solis J., Soriente C., Tsudik G., Uzun E. Using Audio in Secure Device Pairing. *International Journal of Security and Networks*. 2009;4(1):57–68. DOI:10.1504/IJSN.2009.023426

10. Goodrich M.T., Sirivianos M., Solis J., Tsudik G. Uzun E. Loud and Clear: Human-Verifiable Authentication Based on Audio. Distributed Computing Systems. *Proceedings of the 26th International Conference on Distributed Computing Systems, ICDCS 2006, 4–7 July 2006, Lisboa, Portugal*. IEEE; 2006. p.1–10. DOI:10.1109/ICDCS.2006.52

11. Soriente C., Tsudik G., Uzun E. HAPADEP: Human-Assisted Pure Audio Device Pairing. *Proceedings of the 11th International Conference on Information Security, ISC 2008, 15–18 September 2008, Taipei, Taiwan. Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer; 2008. vol.5222. p.385–400. DOI:10.1007/978-3-540-85886-7_27

12. Mayrhofer R. Gellersen H. Shake Well Before Use: Intuitive and Secure Pairing of Mobile Devices. *IEEE Transactions on Mobile Computing.* 2009;8(6):792–806. DOI:10.1109/TMC.2009.51

13. Soriente C., Tsudik G., Uzun E. BEDA: Button-Enabled Device Association. *Proceedings of the 1st International Workshop on Security for Spontaneous Interaction (IWSSI)*. Linz: Institute of Networks and Security; 2007. p.443–449.

14. Kumar A., Saxena N., Tsudik G., Uzun E. Caveat emptor: A comparative study of secure device pairing methods. *Proceedings of the International Conference on Pervasive Computing and Communications, 9–13 March 2009, Galveston, USA*. IEEE; 2009. p.1–10. DOI:10.1109/PERCOM.2009.4912753

15. Korpusov V., Olkhovoy O., Yakovlev V. The Research of the Random Number Generator Based on the Magnetometer. *Proceedings of the VIIth International Conference on Infotelecommunications in Science and Education, 28 February–1 March 2018, St. Petersburg, Russia*. St. Petersburg: The Bonch-Bruevich Saint-Petersburg State University of Telecommunications Publ.; 2018. p.488–494. (in Russ.)

16. Yakovlev V.A. Authentication of Keys Distriburted by the Diffie – Hellman Method for Mobile Devices Based on Authentication Codes and Magnetometric Data. *SPIIRAS Proceedings*. 2019;18(3):705–740. DOI:10.15622/sp.2019.18.3.705-740

17. Maurer U. Information-Theoretically Secure Secret-Key Agreement by not Authenticated Public Discussion. *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, 11–15 May 1997, Konstanz, Germany. Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer; 1997. vol.1233. p.209–223. DOI:10.1007/3-540-69053-0_15

18. Korzhik V., Yakovlev V., Morales-Luna G., Chesnokov R. Perfomance Evaluation of Keyless Authentication Based on Noisy Channel. *Proceedings of the 4th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2007, 13–15 September 2007, St. Petersburg, Russia. Communications in Computer and Information Science*. Berlin, Heidelberg: Springer, 2007. vol.1. p.115–126. DOI:10.1007/978-3-540-73986-9_9

19. Yakovlev V. Authentication Method Diffie-Hellman Values Based on Pre-Distributed Binary Sequences and Strictly Universal Hash Functions // *Proceedings of the* X *International Conference on Infotelecommunications in Science and Education, 24–28 February 2021, St. Petersburg, Russia*. St. Petersburg: The Bonch-Bruevich Saint-Petersburg State University of Telecommunications Publ.; 2021. p. 693–698. (in Russ.)

20. Yakovlev V., Korzhik V., Adadurov S. Authentication of Diffie-Hellman Protocol for Mobile Units Executing a Secure Device Pairing Procedure in Advance. *Proceedings of the 29th Conference of Open Innovations Association, FRUCT, 12–14 May 2021, Tampere, Finland*. IEEE; 2021. DOI:10.23919/FRUCT52173.2021.9435495

21. Wegman M.N., Carter J.L. New Hash Functions and their Use in Authentication and Set Equality. *Journal of Computer and System Sciences*. 1981;22(3):265–279. DOI:10.1016/0022-0000(81)90033-7

22. Carter J.l., Wegman M.N. Universal classes of hash functions. *Journal of Computer and System Sciences*. 1979;18(2):143–154. DOI:10.1016/0022-0000(79)90044-8

23. Maurer U. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*. 1993;39(3):2535–2549.

24. GOST P 34 12-2015. *Information Technology. Cryptographic Information Protection. Block Ciphers*. M.: Standartinform Publ.; 2015. (in Russ.).

25. FIPS 197. Specification for the ADVANCED ENCRIPTION STANDARD (AES). Nov.2001.

Сведения об авторе:

ЯКОВЛЕВ Виктор Алексеевич — доктор технических наук, профессор, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, viyak@bk.ru