(19) Евразийское патентное ведомство

(11) 046054 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2024.02.02

(21) Номер заявки
202392479

(22) Дата подачи заявки
2023.10.03

(51) Int. Cl. ***G06F 21/34*** (2013.01)
G06F 21/42 (2013.01)
G09B 5/04 (2006.01)
H04L 9/14 (2006.01)

(54) СПОСОБ АУТЕНТИФИКАЦИИ ТИФЛОФЛЕШПЛЕЕРА В ОНЛАЙН-БИБЛИОТЕКЕ "ГОВОРЯЩИХ" КНИГ

(43) **2024.01.26**
(96) **2023000160 (RU) 2023.10.03**

(71)(73) Заявитель и патентовладелец:
ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ ЛАБОРАТОРИЯ ЭЛЕКТРОНИКИ "ЭЛЕКЖЕСТ" (RU)

(72) Изобретатель:
Горюнов Михаил Алексеевич (RU)

(74) Представитель:
Луцковский М.Ю., Корниец Р.А. (RU)

(56) US-A1-20110047378
US-A1-20090274303
EA-A1-201990708
US-A1-20160191244

(57) Заявленное изобретение относится к способу и системе аутентификации тифлофлешплеера в онлайн-библиотеке "говорящих книг", который включает в себя обмен данными между тифлофлешплеером (1), сервером (2) выдачи ключей и сервером (3) онлайн-библиотеки. Тифлофлешплеер (1) отправляет уникальный идентификатор (ИУ) серверу (2) выдачи ключей, который генерирует пару из приватного и публичного ключей, шифрует приватный ключ с помощью публичного ключа производителя и отправляет их соответствующим сторонам. Тифлофлешплеер (1) расшифровывает приватный ключ и отправляет ИУ серверу (3) онлайн-библиотеки. Сервер (3) генерирует верный пароль для ИУ, шифрует его и отправляет тифлофлешплееру (1). Тифлофлешплеер (1) расшифровывает пароль и отправляет его серверу (3) для проверки достоверности. Если пароль верен, сервер (3) предоставляет доступ к ресурсам библиотеки и завершает аутентификацию. Заявленные способ и система обеспечивают безопасную и доступную для незрячих людей аутентификацию тифлофлешплеера в онлайн-библиотеке "говорящих книг".

046054 B1

046054 B1

046054 B1

Область техники, к которой относится изобретение

Заявленное изобретение относится к области защиты информации, в частности, к контролю и управлению доступом устройств к информации, в частности, способу аутентификации тифлофлешплеера в онлайн-библиотеке "говорящих" книг для инвалидов по зрению, слепых и слабовидящих.

Предшествующий уровень техники

Тифлофлешплеер представляет собой устройство, предназначенное для воспроизведения "говорящих" книг, то есть книг, репродуцированных в звуковой формат, приспособленное для использования инвалидами по зрению, слепыми и слабовидящими. Формат, определение и распространение "говорящих" книг в России регламентируются ГОСТ Р 59224-2020 "Цифровая "говорящая" книга для слепых и слабовидящих. Технические требования".

С развитием Интернета стали распространены тифлофлешплееры, способные воспроизводить "говорящие" книги не только с локальных носителей информации, но и из онлайн-библиотек "говорящих" книг. При этом заявленный способ аутентификации и аутентификации тифлофлешплеера в онлайн-библиотеке "говорящих" книг используется для ограничения доступа к онлайн-библиотеке "говорящих" книг и предоставления доступа только для легитимных устройств/пользователей.

Таким образом, возникла потребность для аутентификации легитимных тифлофлешплееров на сервере онлайн-библиотеки и предотвращении доступа нелегитимных устройств к нему.

Из уровня техники известны следующие способы и системы аутентификации устройства на целевом сервере, схожие с заявленным изобретением.

Известен ПРОТОКОЛ СЕТЕВОЙ АУТЕНТИФИКАЦИИ KERBEROS [https://web.mit.edu/kerberos/www/kxb5-latest/doc/basic/ccache_def.html], согласно которому используют парные ключи ключей, которыми обмениваются пользователь и сервер для безопасной аутентификации и шифрования данных. Согласно известному способу пользователь, пытающийся получить доступ к ресурсу, отправляет запрос на сервер аутентификации, запрашивая тикет аутентификации (TGT), сервер выдачи ключей проверяет личность пользователя, а затем создает TGT, содержащий зашифрованные данные, включая временную метку и ключ сеанса. Пользователь получает TGT и использует его для запроса нового тикета для доступа к конкретному целевому серверу, который также зашифрован с использованием ключа сеанса пользователя. Целевой сервер проверяет тикет с использованием общего секретного ключа с аутентификационным сервером и если тикет действителен и корректен, сервер предоставляет доступ пользователю.

Протокол Kerberos обладает рядом преимуществ, но также имеет недостатки, снижающие безопасность данного протокола, особенно по сравнению с асимметричным шифрованием. В Kerberos используются симметричные ключи, что означает, что необходим обмен общим секретным ключом. Это представляет серьезную проблему, так как ключ должен быть передан или установлен перед началом обмена данными. Следовательно, это создает потенциально уязвимые точки, где злоумышленники могут перехватывать или скомпрометировать ключ. При этом в известном способе каждая пара сторон должна иметь уникальный секретный ключ для обмена данными, что становится сложным и неэффективным при большом числе пользователей или устройств, так как управление всеми этими ключами становится трудозатратным и неудобным. Кроме того, секретный ключ в известном способе должен быть известен обеим сторонам для расшифровки данных, что создает риски, связанные с утечкой ключей или их компрометацией. При этом, если секретный ключ скомпрометирован, то все прошлые и будущие сообщения, зашифрованные этим ключом, также могут быть скомпрометированы. Поэтому требуется обмен новым секретным ключом, что может быть сложно в реальном времени. И наконец, известный способ не приспособлен для использования слабовидящими и незрячими людьми, поскольку подразумевает ввод текстовых паролей.

Также известны СИСТЕМА И СПОСОБ ДЛЯ АУТЕНТИФИКАЦИИ УСТРОЙСТВ [EA201990708, 2017.09.08], рассматриваемые в качестве наиболее близкого аналога. В известной системе и способе используются временные идентификаторы, генерируемые каждым устройством с использованием динамических и статических состояний. Временные идентификаторы обмениваются и аутентифицируются между устройствами, что позволяет устанавливать доверительные взаимоотношения. В некоторых случаях сервер выдачи ключей может генерировать временный идентификатор для устройства, который затем отправляется или принимается устройством. Устройства могут также устанавливать доверительное взаимоотношение на основе ранее использованного хэша данных, созданного, например, с помощью алгоритма с сохраненным и совместно использованным одноразовым паролем.

Известная система и способ имеет несколько недостатков. Во-первых, использование статических цифровых сертификатов представляет риск безопасности. Поскольку эти сертификаты остаются неизменными, они могут быть скомпрометированы злоумышленниками и использованы для несанкционированного доступа. Во-вторых, генерация и обмен временными идентификаторами требует точной реализации и несоблюдение безопасных методов генерации и хранения временных идентификаторов может привести к уязвимостям в системе. Кроме того, известная система и способ сложны для использования слабовидящими и незрячими людьми, поскольку требуют взаимодействия с цифровыми устройствами и сложных технических процессов, что может создать барьеры для их участия. Важно учесть, что эти не-

достатки не только повышают риск безопасности, но также могут затруднить использование системы для пользователей тифлофлешплееров, то есть слабовидящих и незрячих людей.

Сущность изобретения

С учетом выявленных в уровне техники недостатков, настоящее изобретение направлено на решение технической задачи, заключающейся в создании способа аутентификации тифлофлешплеера в онлайн-библиотеке "говорящих книг" повышенной безопасности, доступного для пользователей тифлофлешплееров, то есть слабовидящих и незрячих людей.

При решении указанной технической задачи обеспечивается достижение технического результата, выражающегося в повышении безопасности способа аутентификации тифлофлешплеера в онлайн-библиотеке "говорящих книг".

Указанную техническую задачу решает и указанный технический результат обеспечивает заявленный способ аутентификации тифлофлешплеера в онлайн-библиотеке "говорящих книг", который задействует тифлофлешплеер, содержащий уникальный идентификатор устройства (ИУ) и приватный ключ производителя тифлофлешплееров (ПрКП), сервер выдачи ключей, содержащий публичный ключ производителя тифлофлешплееров (ПбКП), и по меньшей мере один сервер онлайн-библиотеки, выполненные с возможностью обмена данными, согласно которому: тифлофлешплеер направляет на сервер выдачи ключей свой ИУ; в ответ на получение ИУ тифлофлешплеера, сервер безопасности генерирует пару из приватного ключа тифлофлешплеера (ПрКТ) и публичного ключа тифлофлешплеера (ПбКТ); сгенерированный ПрКТ сервер шифрует с помощью ПбКП и направляет тифлофлешплееру, а сгенерированный ПбКТ направляет указанному по меньшей мере одному серверу онлайн-библиотеки вместе с ИУ; тифлофлешплеер расшифровывает направленный ему ПрКТ с помощью ПрКП; тифлофлешплеер направляет ИУ серверу онлайн-библиотеки в ответ на получение от тифлофлешплеера ИУ, сервер онлайн-библиотеки генерирует верный пароль для полученного ИУ, шифрует его с помощью ПбКТ и направляет тифлофлешплееру, тифлофлешплеер расшифровывает полученный пароль и направляет серверу онлайн-библиотеки ИУ верный пароль; сервер онлайн-библиотеки проверяет достоверность пароля, если установлено, что пароль недостоверный, сервер онлайн-библиотеки повторно генерирует верный пароль, шифрует с помощью ПбКТ и направляет тифлофлешплееру; если установлено, что пароль достоверный, то сервер онлайн-библиотеки предоставляет доступ тифлофлешплееру к ресурсам онлайн-библиотеки и успешно завершает аутентификацию тифлофлешплеера в онлайн-библиотеке.

В частности, сервер выдачи ключей генерирует новую пару ключей ПрКТ и ПбКТ через предварительно заданные промежутки времени и направляет новый ПрКТ тифлофлешплееру в зашифрованном виде, и новый ПбКТ - серверу онлайн-библиотеки.

В частности, сервер выдачи ключей генерирует новую пару ключей ПрКТ и ПбКТ в ответ на обращение тифлофлешплеера с ИУ, по которому уже была выдана пара ключей и направляет новый ПрКТ тифлофлешплееру в зашифрованном виде, и новый ПбКТ - серверу онлайн-библиотеки.

В частности, сервер онлайн-библиотеки сохраняет в памяти хэш-сумму верного пароля, но не сам пароль, и определяет достоверность полученного от тифлофлешплеера пароля сравнением его хэш-суммы с сохраненной хэш-суммой.

В частности, сервер онлайн-библиотеки добавляет к генерируемому паролю соль в виде текущего времени, ИУ тифлофлешплеера или предварительно заданный фрагмент ПбКТ.

Кроме того, указанную техническую задачу решает и указанный технический результат обеспечивает заявленная система аутентификации тифлофлешплеера в онлайн-библиотеке "говорящих книг", которая содержит тифлофлешплеер, содержащий приватный ключ производителя тифлофлешплееров (ПрКП), сервер выдачи ключей, содержащий публичный ключ производителя тифлофлешплееров (ПбКП) и по меньшей мере один сервер онлайн-библиотеки, выполненные с возможностью обмена данными друг с другом и сконфигурированные осуществлять этапы вышеописанного способа.

Перечень фигур чертежей и иных материалов

На фиг. 1 показана блок-схема заявленного способа аутентификации тифлофлешплеера в онлайн-библиотеке "говорящих книг".

На фиг. 2 схематично показана система для осуществления заявленного способа и обмен информацией между ее компонентами в примере осуществления с одной онлайн-библиотекой.

На фигурах обозначены: 1 - тифлофлешплеер; 2 - сервер выдачи ключей; 3 - сервер онлайн-библиотеки.

Сведения, подтверждающие возможность осуществления изобретения

Заявленное изобретение в первом своем аспекте относится к способу аутентификации тифлофлешплеера в онлайн-библиотеке "говорящих" книг.

Согласно заявленному способу, используется тифлофлешплеер 1, который содержит в памяти уникальный идентификатор устройства (ИУ или DID от англ. Device IDentification). Указанный ИУ присваивают тифлофлешплееру 1 на этапе производства и устанавливают его в память тифлофлешплеера. Указанный ИУ предпочтительно представляет собой цифробуквенный код, который далее используют в качестве логина при аутентификации в онлайн-библиотеке.

ИУ присваивается устройству на этапе производства и остается неизменным на протяжении всего

срока службы устройства, что обеспечивает уникальность и неподдельность идентификатора и служит защите от поддельных устройств и манипуляций с идентификационной информацией.

Поскольку ИУ уникален для каждого устройства, это обеспечивает высокий уровень аутентификации при использовании ИУ в качестве логина. Использование предустановленного ИУ в качестве логина при аутентификации имеет особую важность и ценность для слепых и слабовидящих людей, поскольку избавляет их от необходимости вводить логин самостоятельно и взаимодействовать с экраном.

Тифлофлешплеер 1 также содержит в памяти приватный ключ производителя (ПрКП), или приватный ключ первой пары ключей. Указанный ПрКП предпочтительно устанавливают вместе с программным обеспечением тифлофлешплеера. Указанный ПрКП представляет собой закрытый криптографический ключ, который имеется у производителя тифлофлешплееров и который производитель включает в программное обеспечение, устанавливаемое в тифлофлешплеер 1. При этом публичный ключ производителя (ПбКП), или публичный ключ первой пары ключей, хранится на сервере 2 выдачи ключей.

Преимущества конфигурации безопасности, в которой тифлофлешплеер 1 содержит в памяти приватный ключ производителя (ПрКП), а публичный ключ производителя (ПбКП) хранится на сервере 2 выдачи ключей заключаются следующем. Указанная конфигурация позволяет имплементировать двухэтапную аутентификацию, в которой первым фактором является то, что тифлофлешплеер 1 имеет (уникальный ИУ и ПрКП), а вторым - то, что тифлофлешплеер 1 "знает" (ПбКП, размещенный на сервере 2 выдачи ключей и передаваемый им на целевой сервер 3 онлайн-библиотеки), что сильно повышает безопасность, поскольку злоумышленнику для доступа к серверу необходимо будет знать как минимум ИУ, ПрКП и ПрКП, из которых ПрКП и ПБКП не передаются в сети. Кроме того, публичный ключ на сервере может быть заменен или отозван, что делает скомпрометированное устройство бесполезным без доступа к актуальным ключам на сервере. Кроме того, наличие сервера 2 выдачи ключей позволяет более гибко управлять доступом к ресурсам. Администратор системы безопасности может легко отозвать или изменить доступ для конкретных устройств, не затрагивая само программное обеспечение на устройствах пользователей. Таким образом, конфигурация с хранением приватного ключа производителя в устройстве и публичного ключа на сервере безопасности обеспечивает более высокий уровень безопасности, гибкость управления доступом и защиту от компрометации устройств, что делает ее привлекательным выбором для обеспечения безопасности тифлофлешплееров и других аналогичных устройств, а также обеспечивает возможность создания между тифлофлешплеером 1 и сервером 2 выдачи ключей первого одностороннего защищенного канала передачи данных от сервера 2 выдачи ключей к тифлофлешплееру.

Согласно заявленному способу, тифлофлешплеер 1 обращается к серверу 2 выдачи ключей и направляет ему сообщение, содержащее ИУ тифлофлешплеера.

Для каждого ИУ на сервере 2 выдачи ключей хранится или, предпочтительно, генерируется вторая пара ключей - пара из приватного ключа тифлофлешплеера (ПрКТ) и публичного ключа тифлофлешплеера (ПбКТ).

Указанная система защиты с использованием пары ключей известна в уровне техники как ассиметричное шифрование. В паре публичный/приватный ключ публичный ключ используется для шифрования информации, в частности, как более подробно раскрыто далее, на стороне сервера 2 выдачи ключей и сервера 3 онлайн-библиотеки, а приватный ключ используются для расшифровки информации, зашифрованной с помощью соответствующего публичного ключа. Эти ключи математически связаны, но вычисление приватного ключа из публичного ключа является вычислительно сложной и непрактичной задачей.

Далее сервер 2 выдачи ключей направляет на все сервера онлайн-библиотек "говорящих" книг, список адресов которых хранится в памяти сервера 2 выдачи ключей, сообщение для сервера онлайн-библиотек, содержащее ИУ тифлофлешплеера и сгенерированный ПбКТ. Вместе с этим, сервер 2 выдачи ключей направляет на тифлофлешплеер 1 сообщение для тифлофлешплеера, содержащие в себе сгенерированный ПрКТ, зашифрованный с помощью хранящегося или сгенерированного на сервере 2 выдачи ключей ПбКП, то есть, отправляет ПбКТ тифлофлешплееру по указанному первому одностороннему защищенному каналу передачи данных.

Направление на тифлофлешплеер 1 ПрКТ и направление на сервер онлайн-библиотеки ПбКТ обеспечивает возможность создания между тифлофлешплеером 1 и каждым сервером 3 онлайн-библиотеки второй односторонний защищенный канал передачи данных от сервера 3 онлайн-библиотеки к тифлофлешплееру 1.

После получения тифлофлешплеером от сервера 2 выдачи ключей сообщения для тифлофлешплеера, тифлофлешплеер 1 расшифровывает содержащуюся в указанном сообщении зашифрованную информацию о ПрКТ с использованием хранящегося на тифлофлешплеере ПрКП, после чего сохраняет в памяти ПрКТ.

Указанная система безопасности, использующая две пары асимметричных ключей для защиты передачи данных и обеспечения конфиденциальности, в том числе защиты передачи самих ключей, не известна из уровня техники и поэтому нет общепризнанного термина, однозначно характеризующего его. Данный механизм может быть назван системой двухуровневого асимметричного шифрования или системой каскадного асимметричного шифрования, что подчеркивает использование двух слоев или уров-

ней ассиметричного шифрования, где один слой предоставляет доступ ко второму.

Использование двух пар ключей добавляет дополнительный уровень безопасности системе. Приватный ключ первой пары используется для расшифровки сообщения от сервера 2 выдачи ключей, а приватный ключ второй пары будет использоваться для расшифровки данных, отправляемых на сервер 3 онлайн-библиотеки. Это означает, что даже если злоумышленник сможет получить доступ к приватному ключу первой пары на тифлофлешплеере, он все равно не сможет расшифровать данные, передаваемые на целевой сервер, без приватного ключа второй пары.

Кроме того, указанная система обеспечивает безопасное распределение ролей участников способа аутентификации и тифлофлешплеер 1 и сервер 3 онлайн-библиотеки могут установить одностороннее защищенное соединение без передачи приватного ключа в незашифрованном виде, а также позволяет изменять ключи шифрования для каждой сессии или пользователя, что обеспечивает более высокий уровень безопасности и предотвращает возможность перехвата данных злоумышленниками.

В одном опциональным примере осуществления заявленного способа сервер 2 выдачи ключей сконфигурирован генерировать новую пару ключей ПрКТ и ПбКТ через предварительно заданные промежутки времени и направлять на тифлофлешплеер 1 (в зашифрованном виде) и сервера 3 онлайн-библиотеки.

Регулярное обновление пары ключей позволяет скрыть паттерны шифруемых данных и предотвратить их обнаружение. Если злоумышленник сможет захватить и проанализировать трафик, он может заметить повторяющиеся ключи и попытаться использовать это для анализа уязвимостей. Динамическое обновление создает дополнительную неопределенность и делает такой анализ сложнее. Кроме того, обеспечивается сокращение времени экспозиции, то есть, даже если ПрКТ был скомпрометирован, динамическое обновление ключей ограничивает время, в течение которого злоумышленник может использовать этот ключ и например, создать нелигитимную копию тифлофлешплеера. Поскольку ключи обновляются через определенные временные интервалы, даже в случае компрометации, злоумышленник может иметь доступ только к данным, зашифрованным с использованием устаревшего ключа, что в целом повышает сложность и ресурсозатратность атак, поскольку для успешной атаки злоумышленнику необходимо не только скомпрометировать текущую пару ключей ПрКТ+ПбКТ, но и следить за регулярными обновлениями и адаптировать свои атаки к новым парам ключам.

В другом опциональном примере осуществления заявленного способа сервер 2 выдачи ключей сконфигурирован генерировать новую пару ключей ПрКТ и ПбКТ в случае выявления первичного обращения тифлофлешплеера 1 с ИУ, по которому уже была выдана пара ключей. Данное событие может свидетельствовать о попытке аутентификации нелегитимной копии тифлофлешплеера.

Тифлофлешплеер 1 устанавливает соединение с сервером 3 онлайн-библиотеки и передает сообщение для сервера 3 онлайн-библиотеки, содержащее свой ИУ и временный пароль, предустановленный в тифлофлешплеере. Данный пароль не является верным и предназначен лишь для информирования онлайн-библиотеки об отсутствии верного пароля на тифлофлешплеере.

В ответ на установление первого соединения, сервер 3 онлайн-библиотеки, генерирует верный пароль для полученного ИУ и сохраняет в памяти его хэш-сумму, при этом сам пароль доступа тифлофлешплеера 1 к онлайн-библиотеке не сохраняется в памяти сервера 3 онлайн-библиотеки.

Для получения хэш-суммы используют известный из уровня техники алгоритм хэширования: MD5, SHA-256, SHA-3, BCrypt, Argon2 или Scrypt.

Для генерирования пароля сервером 3 онлайн-библиотеки может использоваться генерирование случайной последовательности символов предварительно заданной длины.

Опционально, сервер 3 онлайн-библиотеки сконфигурирован добавлять к генерируемому паролю соль (salt), то есть случайной уникальной строки, перед его хэшированием. В качестве соли может использоваться текущее время, ИУ тифлофлешплеера 1 или предварительно заданный фрагмент ПбКТ, например, первые пять символов ПбКТ, что обеспечивает дополнительный слой безопасности, поскольку злоумышленникам потребуется дополнительное время и усилия для атаки каждого хэша или знание ПбКТ.

Использование соли обеспечивает повышение безопасности за счет усиления пароля, в частности, соль делает каждый хэш уникальным для заданного времени или для заданного тифлофлешплеера 1 с уникальным ИУ, даже если для них генерируется один и тот же пароль, то есть, хэши паролей не повторяются в базе данных, что делает атаки по словарю менее эффективными, при этом увеличивается сложность вычисления пароля и повышает безопасность в случае утечки данных.

При этом сервер 3 онлайн-библиотеки сконфигурирован хранить в памяти не пароль доступа тифлофлешплеера 1, а хэш-сумму указанного пароля, которую он сконфигурирован сравнивать с хэш-суммой пароля, полученного от тифлофлешплеера 1 для определения подлинности комбинации ИУ и пароля. Опционально, сервер 3 онлайн-библиотеки сконфигурирован хранить в памяти зашифрованный с помощью ПбКТ пароль.

Хранение пароля на сервере 3 онлайн-библиотеки в виде его хэш-суммы, а не в явном виде способствует повышению безопасности пароля и предотвращению их утечки в случае компрометации сервера 3 онлайн-библиотеки или ее базы данных. В частности, это обеспечивает защита от компрометации, по-

скольку в случае получения доступа к серверу злоумышленники увидят только нечитаемую строку (хэш), которую сложно или практически невозможно преобразовать обратно в исходный пароль. Кроме того, обеспечивает защита паролей от доступа персонала, обслуживающего сервер 3 онлайн-библиотеки, что уменьшает риск недобросовестного использования или утечки паролей.

В ответ на получение сервером 3 онлайн-библиотеки от тифлофлешплеера 1 сообщения для сервера 3 онлайн-библиотеки, последний проверяет подлинность полученной комбинации ИУ и пароля, посредством сравнения хэш-суммы полученного пароля с хранящейся в памяти хэш-суммой.

Если сервер 3 онлайн-библиотеки устанавливает, что полученный пароль не является достоверным, сервер 3 онлайн-библиотеки возвращает тифлофлешплееру сообщение для тифлофлешплеера 1 с информацией о верном пароле соответствующего ИУ, зашифрованное с использованием ПбКТ.

Шифрование пароля обеспечивает дополнительный барьер для аутентификации, и злоумышленники, имеющие доступ к серверу или базе данных, не могут прочитать пароль напрямую, даже если они скомпрометировали хранилище паролей; снижение риска перехвата пароля; обеспечивает дополнительную аутентификацию клиента, поскольку требует для расшифровки ПрКТ, установленного на тифлофлешплеере, который мог быть получен им только в случае предварительного успешного установления первого одностороннего защищенного канала передачи данных с сервером 2 выдачи ключей.

Направление пароля клиенту (тифлофлешплееру) от целевого сервера (сервер 3 онлайн-библиотеки), доступ к которому запрашивается клиентом, является крайне неочевидным решением в области аутентификации устройств и не используется в области защиты информации из-за своей очевидной небезопасности. Действительно, злоумышленник сравнительно просто может выдать себя за легитимного пользователя и получить от целевого сервера требуемый пароль для доступа к нему, поэтому данный способ не используется в известных из уровня техники системах безопасности. Однако, указанный недостаток низкой безопасности полностью устранен в описываемом способе за счет использования вышеописанной каскадной системы аутентификации, в которой только легитимный тифлофлешплеер, обладающий ПрКП и ПрКТ, соответствующим его уникальному ИУ, может расшифровать пароль от сервера 3 онлайн-библиотеки. С учетом устранения вышеуказанного недостатка, отправка пароля клиенту целевым сервером обеспечивает следующие преимущества:

во-первых, отправка сервером 3 онлайн-библиотеки пароля избавляет пользователя от необходимости ввода и запоминания пароля и избавляет его от необходимости взаимодействия с экраном и графическим интерфейсом, что особенно предпочтительные для использующих тифлофлешплееры инвалидов по зрению, слепых и слабовидящих. Во-вторых, отправка сервером 3 онлайн-библиотеки пароля повышает безопасность пароля за счет возможность генерирования сильных сложных паролей, например, с использованием соли, а также реализовать динамическое изменение пароля через предварительно заданные промежутки времени или в ответ на наступление определенных событий, как боле подробно раскрыто далее.

В ответ на получение тифлофлешплеером сообщения от сервера 3 онлайн-библиотеки для тифлофлешплеера 1, последний расшифровывает содержащуюся в сообщении зашифрованную информацию о верном пароле с использованием ПрКТ и заменяет временный пароль в своей памяти на верный пароль.

Тифлофлешплеер 1 устанавливает повторное соединение с сервером 3 онлайн-библиотеки и передает в него сообщение для сервера 3 онлайн-библиотеки, содержащее свой ИУ и верный пароль, сохраненный в тифлофлешплеере. В ответ на получение сервером 3 онлайн-библиотеки от тифлофлешплеера 1 сообщения для сервера 3 онлайн-библиотеки, последний проверяет подлинность полученной комбинации ИУ и пароля. Если сервер 3 онлайн-библиотеки устанавливает, что полученный пароль соответствует верному паролю для данного ИУ, сервер 3 онлайн-библиотеки предоставляет доступ тифлофлешплееру к ресурсам 3 онлайн-библиотеки и успешно завершает аутентификацию тифлофлешплеера 1 в онлайн-библиотеке. Если же сервер 3 онлайн-библиотеки устанавливает недостоверность полученного сочетания ИУ и пароля, он генерирует новый пароль.

Доступ ко всем ресурсам онлайн-библиотеки с помощью тифлофлешплеера 1 предоставляется исключительно зарегистрированным читателям этой библиотеки. Для этого пользователь тифлофлешплеера 1 должен пройти процедуру регистрации в библиотеке с указанием ИУ своего тифлофлешплеера 1. Контроль доступа тифлофлешплееров по ИУ к онлайн-библиотекам осуществляется сотрудниками этих библиотек.

Таким образом, согласно предложенному способу аутентификации, только легитимный тифлофлешплеер, обладающий как приватным ключом производителя ПрКП, так и приватным ключом тифлофлешплеера ПрКТ может получить и расшифровать верный пароль.

Сервер 3 онлайн-библиотеки сконфигурирован периодически обновлять пароль для определенного ИУ с определенной периодичностью, например, каждые 5 часов, то есть периодически генерировать новый верный пароль, что приводит к выявлению недостоверности прежнего пароля и отправке нового верного пароля тифлофлешплееру с определенным ИУ.

Динамическая смена пароля способствует увеличению безопасности аутентификации, в частности, уменьшает время действия украденных паролей, и если злоумышленнику станет доступен украдет пароль тифлофлешплеера, динамическая смена пароля ограничивает его эффективность во времени; защи-

щает пароль по времени от атак методом перебора паролей (брутфорс).

Заявленное изобретение во втором своем аспекте относится к системе аутентификации тифлофлешплеера в онлайн-библиотеке "говорящих" книг, предназначенной для осуществления вышеописанного способа.

Как показано на фиг. 2, система аутентификации тифлофлешплеера в онлайн-библиотеке, предназначенная для осуществления вышеописанного способа, включает тифлофлешплеер 1, содержащий приватный ключ производителя тифлофлешплееров (ПрКП), сервер 2 выдачи ключей, содержащий публичный ключ производителя тифлофлешплееров (ПбКП) и по меньшей мере один сервер 3 онлайн-библиотеки, выполненные с возможностью обмена данными друг с другом, например, посредством глобальной сети Интернет.

Тифлофлешплеер - это устройство, предназначенное для воспроизведения аудиокниг и других аудиофайлов, специально разработанное для использования слабовидящими и незрячими людьми. По указанной причине тифлофлешплееры не оснащены экранами и клавиатурами, приспособленными для ввода логина и пароля.

В указанной системе тифлофлешплеер 1, сервер 2 выдачи ключей и сервер 3 онлайн-библиотеки сконфигурированы с возможностью осуществления этапов вышеописанного способа.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ аутентификации тифлофлешплеера в онлайн-библиотеке "говорящих книг", который задействует выполненные с возможностью обмена данными друг с другом тифлофлешплеер, содержащий уникальный идентификатор устройства (ИУ) и приватный ключ производителя тифлофлешплееров (ПрКП), сервер выдачи ключей, содержащий публичный ключ производителя тифлофлешплееров (ПбКП), и по меньшей мере один сервер онлайн-библиотеки, и согласно которому:

тифлофлешплеер направляет на сервер выдачи ключей свой ИУ;

в ответ на получение ИУ тифлофлешплеера, сервер безопасности генерирует пару из приватного ключа тифлофлешплеера (ПрКТ) и публичного ключа тифлофлешплеера (ПбКТ);

сгенерированный ПрКТ сервер шифрует с помощью ПбКП и направляет тифлофлешплееру, а сгенерированный ПбКТ направляет указанному по меньшей мере одному серверу онлайн-библиотеки вместе с ИУ тифлофлешплеера;

тифлофлешплеер расшифровывает направленный ему ПрКТ с помощью ПрКП;

тифлофлешплеер направляет ИУ серверу онлайн-библиотеки;

в ответ на получение от тифлофлешплеера ИУ, сервер онлайн-библиотеки генерирует верный пароль для полученного ИУ, шифрует его с помощью ПбКТ и направляет тифлофлешплееру,

тифлофлешплеер расшифровывает полученный пароль с помощью ПрКТ и направляет его серверу онлайн-библиотеки со своим ИУ;

сервер онлайн-библиотеки проверяет достоверность пароля,

если установлено, что пароль недостоверный, сервер онлайн-библиотеки повторно генерирует верный пароль, шифрует с помощью ПбКТ и направляет тифлофлешплееру;

если установлено, что пароль достоверный, то сервер онлайн-библиотеки предоставляет доступ тифлофлешплееру к ресурсам онлайн-библиотеки и успешно завершает аутентификацию тифлофлешплеера в онлайн-библиотеке.

2. Способ по п.1, в котором сервер выдачи ключей генерирует новую пару ключей ПрКТ и ПбКТ через предварительно заданные промежутки времени и направляет новый ПрКТ тифлофлешплееру в зашифрованном виде, и новый ПбКТ - серверу онлайн-библиотеки.

3. Способ по п.1, в котором сервер выдачи ключей генерирует новую пару ключей ПрКТ и ПбКТ в ответ на обращение тифлофлешплеера с ИУ, по которому уже была выдана пара ключей и направляет новый ПрКТ тифлофлешплееру в зашифрованном виде, а новый ПбКТ - серверу онлайн-библиотеки.

4. Способ по п.1, в котором сервер онлайн-библиотеки сохраняет в памяти хэш-сумму верного пароля, но не сам пароль, и определяет достоверность полученного от тифлофлешплеера пароля, сравнивая его хэш-сумму с сохраненной хэш-суммой.

5. Способ по п.1, в котором сервер онлайн-библиотеки добавляет к генерируемому паролю соль в виде текущего времени, ИУ тифлофлешплеера или предварительно заданный фрагмент ПбКТ.

6. Система аутентификации тифлофлешплеера в онлайн-библиотеке "говорящих книг", которая содержит тифлофлешплеер, содержащий приватный ключ производителя тифлофлешплееров (ПрКП), сервер выдачи ключей, содержащий публичный ключ производителя тифлофлешплееров (ПбКП) и по меньшей мере один сервер онлайн-библиотеки, выполненные с возможностью обмена данными друг с другом и сконфигурированные осуществлять этапы способа по п.1.

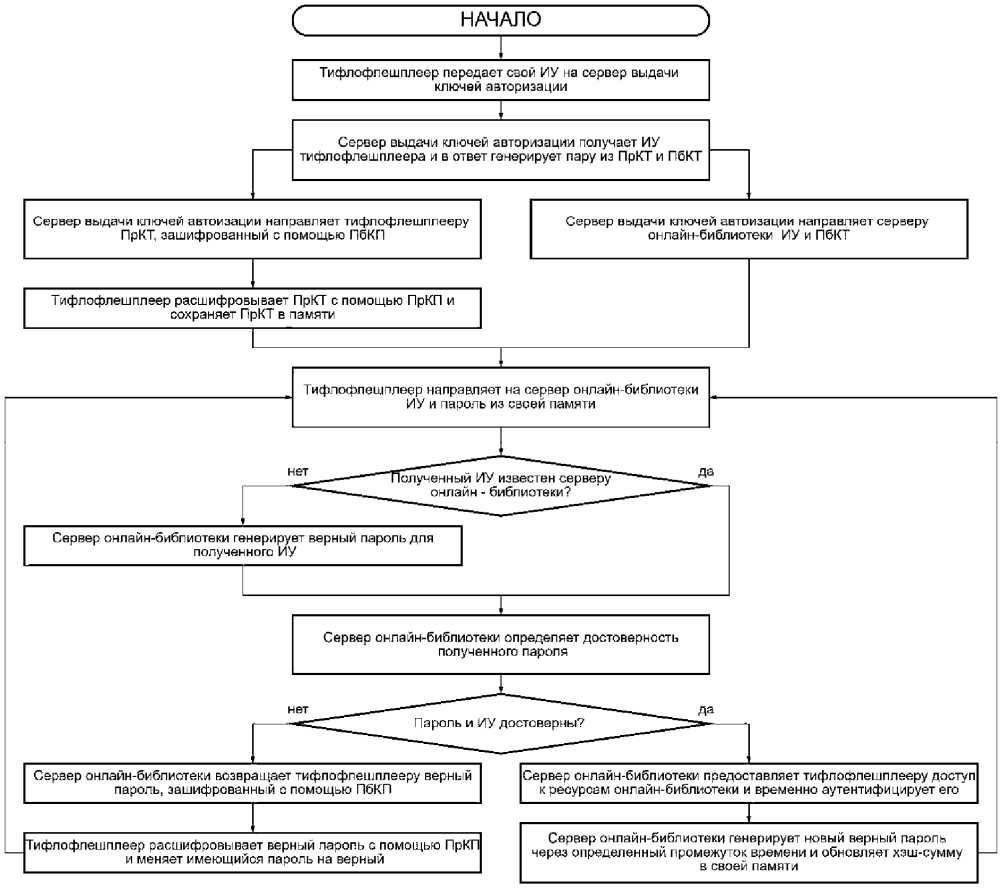
7. Система по п.6, в которой сервер выдачи ключей конфигурирован генерировать новую пару ключей ПрКТ и ПбКТ через предварительно заданные промежутки времени и направляет новый ПрКТ тифлофлешплееру в зашифрованном виде, а новый ПбКТ - серверу онлайн-библиотеки.

8. Система по п.6, в которой сервер выдачи ключей конфигурирован генерировать новую пару клю-

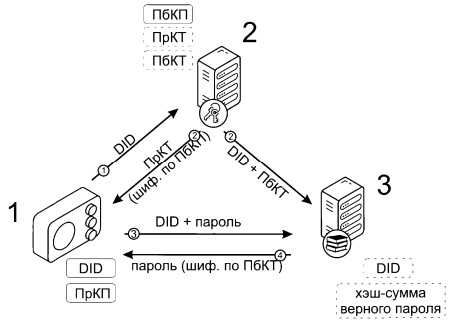
чей ПрКТ и ПбКТ в ответ на обращение тифлофлешплеера с ИУ, по которому уже была выдана пара ключей, и направлять новый ПрКТ тифлофлешплееру в зашифрованном виде, и новый ПбКТ - серверу онлайн-библиотеки.

9. Система по п.6, в которой сервер онлайн-библиотеки конфигурирован сохранять в памяти хэш-сумму верного пароля, но не сам пароль, и определять достоверность полученного от тифлофлешплеера пароля посредством сравнения его хэш-суммы с сохраненной хэш-суммой.

10. Система по п.6, в которой сервер онлайн-библиотеки конфигурирован добавлять к генерируемому паролю соль в виде текущего времени, ИУ тифлофлешплеера или предварительно заданный фрагмент ПбКТ.



Фиг. 1



Фиг. 2