(19) Евразийское патентное ведомство

(11) 034474 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2020.02.12

(21) Номер заявки
201491905

(22) Дата подачи заявки
2012.04.20

(51) Int. Cl. *H04L 9/32* (2006.01)

(54) СПОСОБ И СИСТЕМА ДЛЯ АБСТРАКТНЫХ И РАНДОМИЗИРОВАННЫХ ОДНОРАЗОВЫХ ПАРОЛЕЙ ДЛЯ ТРАНЗАКЦИОННОЙ АУТЕНТИФИКАЦИИ

(43) **2015.03.31**
(86) **PCT/IB2012/052006**
(87) **WO 2013/061171 2013.05.02**

(71)(73) Заявитель и патентовладелец:
ФОРТИКОД ЛИМИТЕД (AU)

(72) Изобретатель:
Смейлз Энтони (AU)

(74) Представитель:
Медведев В.Н. (RU)

(56) US-B2-8041954
US-B2-8042159
US-A1-20110197266

(57) Раскрыты система обеспечения безопасности и способ для аутентификации доступа пользователя в систему. Система обеспечения безопасности принимает от пользователя запрос аутентификации и отвечает, создавая матрицу обеспечения безопасности на основе сохраненных ранее пользовательского ключевого слова и данных о пользовательских предпочтениях, причем матрица обеспечения безопасности отличается для каждого запроса аутентификации. Система обеспечения безопасности отправляет пользователю матрицу обеспечения безопасности и ожидает одноразовый код в ответ на матрицу обеспечения безопасности. Пользователь формирует одноразовый код на основе пользовательского ключевого слова, пользовательских предпочтений и матрицы обеспечения безопасности. Система обеспечения безопасности проверяет одноразовый код с использованием матрицы обеспечения безопасности, ключевого слова и пользовательских предпочтений и отвечает, отправляя пользователю результат аутентификации, который либо разрешает, либо запрещает доступ в систему. Дополнительно система обеспечения безопасности отправляет сообщение о выполнении или невыполнении в систему, доступ к которой должен быть осуществлен.

034474 B1

034474 B1

Область техники, к которой относится изобретение

Настоящее изобретение относится в целом к системам и способам аутентификации и, в частности, касается систем аутентификации, отличающихся высокой надежностью.

Описание связанного уровня техники

Обеспечение безопасности персональных идентификационных данных стало краеугольным камнем всех транзакций в современном электронном мире, характеризующемся высокими уровнями инвестиций, вкладываемых в разработку методов обеспечения безопасности и аутентификации, технологии их поддержки, а также в хакерство в этой сфере. Почти все в мире банковских операций зависит от предварительно размещенного персонального идентификационного номера (PIN), который представляет собой секретный числовой пароль, совместно используемый пользователем и системой для аутентификации пользователя в системе, в то время как большинство электронных систем с полнотекстовыми интерфейсами зависят от паролей.

В настоящее время общепринято полностью полагаться на криптографические хэш-функции (CHF). В этих детерминированных процедурах берутся произвольные данные, на основе которых получают вычисленное математическим путем значение хэш-функции, уникальное для этих данных. Хорошо документированным примером функции CHF является алгоритм MD5. Хэш-функции и интеллектуальные способы обеспечения безопасности между клиентом и сервером затрудняют обратное создание индивидуального пароля или PIN-кода на основе копии упомянутых данных. Однако при использовании визуального отслеживания вместе с технологиями фишинга большинство паролей или PIN-кодов можно рассекретить, что позволяет выполнять обработку для мошеннических транзакций. Такими образом, желательно иметь такую схему обеспечения безопасности, которая снижает вероятность возможного рассекречивания аутентификации.

Сущность изобретения

Один вариант осуществления настоящего изобретения представляет собой способ для абстрагирования взаимодействия с клиентским интерфейсом, заключающегося в том, что каждый раз, когда пользователь захочет выполнить аутентификацию в защищенной системе, эта система предоставляет пользователю одноразовый рандомизированный набор символов или чисел в таком виде, который позволяет ему использовать заранее определенное ключевое слово для определения PIN-кода, соответствующего упомянутому рандомизированному ключевому слову.

В частности, один вариант осуществления настоящего изобретения относится к способу проверки аутентичности пользователя для доступа в защищенную систему. Способ включает в себя следующие этапы: прием от пользователя запроса аутентификации, создание матрицы обеспечения безопасности на основе ID пользователя и данных о пользовательских предпочтениях и отправку упомянутой матрицы пользователю, прием от пользователя одноразового кода в ответ на матрицу обеспечения безопасности, проверку правильности одноразового кода на основе матрицы обеспечения безопасности, ID пользователя, по меньшей мере одного пользовательского ключевого слова и данных о пользовательских предпочтениях после проверки правильности одноразового кода, отправку пользователю результата аутентификации, упомянутый результат аутентификации основан на одноразовом коде, матрице обеспечения безопасности, ID пользователя, пользовательском ключевом слове; и отправку сообщения о выполнении или невыполнении на основе результата аутентификации.

Еще один вариант осуществления настоящего изобретения относится к системе обеспечения безопасности, предназначенной для проверки аутентичности пользователя для доступа в защищенную систему. Система обеспечения безопасности включает в себя компьютер для обеспечения безопасности и клиентский интерфейс. Компьютер для обеспечения безопасности запрограммирован для сохранения пользовательского ключевого слова и данных о пользовательских предпочтениях с целью приема от пользователя запроса аутентификации, включающего в себя ID пользователя, для доступа в защищенную систему и создания матрицы обеспечения безопасности в ответ на упомянутый запрос аутентификации на основе сохраненных данных о пользовательских предпочтениях и ID пользователя, для отправки матрицы обеспечения безопасности пользователю и приема от пользователя одноразового кода, для проверки правильности одноразового кода с использованием созданной матрицы обеспечения безопасности, пользовательского ключевого слова и данных о пользовательских предпочтениях, и для отправки пользователю результата аутентификации на основе проверки подлинности, и для отправки в защищенную систему сообщения о выполнении или невыполнении в зависимости от результата аутентификации. Клиентский интерфейс позволяет пользователю передать в систему обеспечения безопасности запрос аутентификации для доступа в защищенную систему, а также принимать и отображать матрицу обеспечения безопасности и дает возможность пользователю отправлять в систему обеспечения безопасности одноразовый код.

Согласно настоящему способу отсутствует корреляция между ключевым словом пользователя и матрицей обеспечения безопасности, предоставляемой пользователю для проверки подлинности. Система обеспечения безопасности формирует случайным образом матрицу обеспечения безопасности, а пользователь использует эту матрицу обеспечения безопасности для определения одноразового кода, являющегося действительным для данного пользователя и данной матрицы обеспечения безопасности. Каждый

запрос аутентификации приводит к созданию новой матрицы обеспечения безопасности, вычисляемой таким образом, чтобы гарантировать минимальную вероятность определения ключевого слова.

Настоящее изобретение открывает новый подход к обеспечению безопасности аутентификации, позволяя пользователю определить одно или более ключевых слов, которые затем использует в качестве персональной ссылки, что дает возможность пользователю создать одноразовый код из рандомизированной матрицы обеспечения безопасности, созданной системой. Ключевое слово никогда непосредственно не вводится во время процесса аутентификации на любой его стадии и, следовательно, никогда не может быть раскрыто или использоваться совместно с каким-либо другим пользователем.

Благодаря разделению процесса аутентификации на три фазы: (i) запрос аутентификации, (ii) подтверждение полномочий и (iii) передача деталей авторизации формируется способ обеспечения безопасности, который может просматривать, записывать и анализировать все транзакционные запросы аутентификации между пользователем, клиентским интерфейсом и системой обеспечения безопасности, с гарантией невозможности идентификации ключевого слова пользователя.

Уровень сложности матрицы обеспечения безопасности может быть изменен пользователем с целью упрощения или усложнения ее определения, но не системой, в которой аутентифицируется пользователь.

Способ по настоящему изобретению можно применить к любой системе, предъявляющей требование, состоящее в том, чтобы аутентификация пользователя выполнялась с минимальными изменениями в защищенной системе или с минимальными изменениями наработанных навыков пользователя. Поскольку матрица обеспечения безопасности и одноразовый код полностью абстрагированы от ключевого слова, требования по обеспечению безопасности никоим образом не влияют на их кодирование для передачи в любом направлении. Таким образом, способ по настоящему изобретению хорошо подходит к любой системе, где есть возможность легко контролировать или следить за соединением между клиентским интерфейсом и защищенной системой.

Указанный способ можно реализовать для одной системы, множества систем или в виде унифицированной общедоступной системы проверки правильности, причем этот способ блокирует любую транзакцию, которая требует от пользователя проверку его идентичности.

Краткое описание чертежей

Эти и другие признаки, аспекты и преимущества настоящего изобретения станут более понятными при обращении к нижеследующему описанию, прилагаемой формуле изобретения и сопроводительным чертежам, на которых

фиг. 1 - запрос аутентификации;

фиг. 2 - запрос проверки подлинности;

фиг. 3 - первый пример одноразового кода, в котором использован сдвиг;

фиг. 4 - второй пример одноразового кода, в котором использованы сдвиг и обход;

фиг. 5 - третий пример одноразового кода, в котором использован обход (индексирование);

фиг. 6 - четвертый пример одноразового кода, в котором использован скачок;

фиг. 7A - примерная архитектура внутреннего сервера обеспечения безопасности для локальной аутентификации;

фиг. 7B - части клиентского интерфейса во время процесса аутентификации;

фиг. 8 - пример архитектуры внутреннего сервера обеспечения безопасности для удаленной Web-аутентификации;

фиг. 9 - пример архитектуры внешнего сервера обеспечения безопасности для удаленной Web-аутентификации;

фиг. 10 - примерная архитектура внутреннего сервера обеспечения безопасности для внутренней и внешней Web-аутентификации и внутренней системной аутентификации;

фиг. 11 - описание структуры сообщений;

фиг. 12 - пользовательские предпочтения;

фиг. 13 - предпочтения защищенной системы;

фиг. 14 - блок-схема варианта осуществления настоящего изобретения и

фиг. 15 - блок-схема варианта для создания и отправки одноразового кода.

Подробное описание изобретения

В последующем описании используются следующие определения.

Защищенная система 20 - это система, требующая от пользователя аутентификацию как предпосылку для обработки транзакций или информационных запросов.

Система 30 обеспечения безопасности - это система, в которой сохраняются ключевое слово и предпочтения пользователя, пользовательские предпочтения и предпочтения систем обеспечения безопасности, и где выполняется обработка для интерфейсов систем обеспечения безопасности.

11 - Запрос аутентификации

31 - Матрица обеспечения безопасности

12 - Одноразовый код

32 - Результат аутентификации

33 - Сообщение о выполнении

Предпочтения 40 пользователя определены в табл. 3, причем они сохраняются внутренне системой 30 обеспечения безопасности.

Ключевое слово 41 представляет собой линейную строку алфавитных символов, которая определена пользователем 10. В приведенных примерах ключевое слово ограничено только алфавитными символами (от A до Z); однако данный способ и система поддерживают алфавитные (в зависимости или независимо от ситуации), числовые, специальные символы или любую их комбинацию.

Предпочтения 50 защищенной системы определены в табл. 4, причем они сохраняются внутри системы 30 обеспечения безопасности.

Клиентский интерфейс 60 представляет собой человеко-машинный интерфейс (HMI), где пользователю 10 требуется использовать клавиатуру, сенсорный экран, клавиатуру для ввода PIN-кода или другое устройство ввода для предоставления Интернет-службе деталей аутентификации (например, банковский автомат или экран входа в систему).

На фиг. 1 пользователь 10 заранее предоставил системе 30 обеспечения безопасности свои предпочтения 40 и свое ключевое слово. Ключевое слово 41 сохраняется в зашифрованном виде в системе 30 обеспечения безопасности и никогда не передается никакой функцией.

На фиг. 1 пользователь выполняет запрос аутентификации на клиентском интерфейсе 60, который, в свою очередь, отправляет запрос 11 аутентификации в защищенную систему 20, которая направляет запрос 11 аутентификации в систему 30 обеспечения безопасности.

На фиг. 2 данные 50 о предпочтениях защищенной системы используются для определения требуемого формата и ограничений клиентского интерфейса 60. Данные 40 о пользовательских предпочтениях используются для определения уровня сложности матрицы 11 обеспечения безопасности, предпочитаемого пользователем 10. Система 30 обеспечения безопасности создает матрицу 31 обеспечения безопасности и отправляет ее обратно в защищенную систему 20 обеспечения безопасности, которая затем направляет матрицу 31 обеспечения безопасности непосредственно на клиентский интерфейс 60 или использует информацию в ней для построения пользовательского представления матрицы 31 обеспечения безопасности, которое затем предоставляется пользователю 10. Формат идентификатора (ID) пользователя не зависит от системы и может представлять собой любой уникальный ID для всех систем, поддерживаемых сервером обеспечения безопасности. Примерами ID пользователя являются ID клиента или адрес электронной почты.

На фиг. 2 пользователь 10 выполняет аутентификацию, используя предоставленную матрицу 31 обеспечения безопасности, для определения одноразового кодового числа 12 путем применения пользовательских предпочтений 40 в сочетании с ключом 41. Это одноразовое кодовое число 12 вводится в клиентский интерфейс 60, который затем посылает его в защищенную систему 20 обеспечения безопасности, а затем в систему 30 обеспечения безопасности, где система 30 обеспечения безопасности проверяет подлинность, используя данные матрицы 31 обеспечения безопасности вместе с одноразовым кодом 12, сохраненным ключевым словом 41 пользователя 10 и предпочтениями 40 пользователя. В ответ на упомянутый запрос система 30 обеспечения безопасности отправляет результат 32 аутентификации обратно в защищенную систему 20, которая посылает его обратно на клиентский интерфейс 60. Одновременно возникает второе взаимодействие, при котором система 30 обеспечения безопасности после успешной аутентификации инициирует отправку сообщения 33 о выполнении в точку уведомления о выполнении системы 30 обеспечения безопасности, как подробно указано в предпочтениях 50 защищенной системы.

Каждый запрос 11 аутентификации и каждая проверка правильности одноразового кода 12 приводит к созданию матрицы 31 обеспечения безопасности на основе повторной рандомизации для предотвращения повторного использования кода 12. Для ограничения максимального количества попыток в данном временном кадре поддерживается регистрация запросов 11 аутентификации и запросов одноразового кода 12, чтобы предотвратить атаку методом прямого перебора кодов и обеспечить звуковое сопровождение указанных попыток.

В примере на фиг. 3 показаны матрица 31 обеспечения безопасности, данные 40 о пользовательских предпочтениях и пользовательское ключевое слово 41. Пользователь 10 использует свое ключевое слово и данные 40 о пользовательских предпочтениях для создания одноразового кода 12.

В данном примере пользователь 10 предпочитает, чтобы:

(a) матрица 31 обеспечения безопасности отображалась в алфавитном порядке и

(b) к отображенной цифре, которая соответствует букве ключевого слова, добавлялась 1.

Значения в матрице для каждого символа ключевого слова порождает 17572. Добавление сдвига, равного +1, к результирующему значению матрицы дает значение 28683 в качестве одноразового кода 12.

В качестве примера на фиг. 4 показаны матрица 31 обеспечения безопасности, пользовательские предпочтения 40 и пользовательское ключевое слово 41. Пользователь 10 использует свое ключевое слово и свои пользовательские предпочтения 40 для создания одноразового кода 12.

Пользовательские предпочтения 10 в данном примере выглядят следующим образом:

(a) матрица 31 обеспечения безопасности должна отображаться в случайном порядке;

(b) добавлять 1 к цифре, отображаемой против буквы ключевого слова; и

(c) добавлять сверх того 3 к первой букве ключевого слова, добавлять сверх того 6 ко второй букве ключевого слова и т.д.

Определив значение в матрице для каждого символа ключевого слова, получим 28672. Добавив сдвиг +1, получим 39783. Добавив обход +3, получим 65608, представляющее собой одноразовый код.

Заметим, что суммирование в данном примере выполняется по модулю десять, хотя можно использовать суммирование по любому модулю.

В качестве примера на фиг. 5 показаны матрица 31 обеспечения безопасности, пользовательские предпочтения 40 и пользовательское ключевое слово 41. Пользователь 10 использует свое ключевое слово и пользовательские предпочтения 40 для создания одноразового кода 12.

Пользовательские предпочтения 40 в данном примере выглядят следующим образом:

(a) матрица 31 обеспечения безопасности должна отображаться в случайном порядке;

(b) добавлять 2 к первой букве ключевого слова, 4 - ко второй букве ключевого слова и т.д.; и

(c) вторая и четвертая цифры в этом примере должны представлять цифры, выбранные пользователем, а ответ с числами для одноразового действительного кода представляет собой:

a. 41215

b. 42225

c. 43235

d. 41235

e. 49285

f. и т.д. - причем релевантными являются только первое, третье и пятое числа.

Определив значение в матрице для каждого символа ключевого слова, получим 2#8#9. Добавив обход +2, получим 4#2#5, представляющее одноразовый код. Опять же заметим, что суммирование представляет собой суммирование по модулю 10.

В качестве примера на фиг. 6 показаны матрица 31 обеспечения безопасности, пользовательские предпочтения 40 и пользовательское ключевое слово 41. Пользователь 10 использует свое ключевое слово и пользовательские предпочтения 40 для создания одноразового кода 12.

Пользовательские предпочтения 10 в данном примере выглядят следующим образом:

(a) матрица 31 обеспечения безопасности должна отображаться в случайном порядке;

(b) добавлять 1 к первой букве ключевого слова, вычитать 1 из второй буквы ключевого слова, добавлять 1 к третьей букве ключевого слова и т.д.

Определив значение матрицы для каждого символа ключевого слова, получим 98428. Добавив скачок +1, получим 07519, представляющее одноразовый код. Опять же, сложение или вычитание представляет собой сложение или вычитание по модулю 10.

На фиг. 7A представлена система 30 обеспечения безопасности, используемая защищенной системой 20 для проверки правильности авторизации пользователей 60, которые входят через локальную сеть 70, к которой подключен пользователь через беспроводной приемопередатчик 72 с использованием проводного или беспроводного соединения.

Этап 1: Пользователь осуществляет доступ в портал входа в защищенную систему - только по запросу для предоставления ID пользователя, который может представлять собой адрес электронной почты, согласно ссылочным позициям 82 и 84 на фиг. 7B.

Этап 2: Пользователь вводит ID пользователя, как показано под ссылочной позицией 84 на фиг. 7B.

Этап 3: Защищенная система отправляет ID пользователя и ID системы в систему обеспечения безопасности, которая выполняет проверку подлинности и возвращает матрицу 31 обеспечения безопасности (смотри 86 на фиг. 7B), которая затем отображается защищенной системой 20 пользователю 60.

Этап 4: Пользователь вводит одноразовый код 12 и входит в систему как нормальный пользователь (86 на фиг. 7B). Система 20 обеспечения безопасности отправляет одноразовый код 12, ID пользователя и ID системы в систему 30 обеспечения безопасности, которая проверяет упомянутый код и предоставляет защищенной системе 20 ID сеанса, если упомянутый код прошел проверку подлинности.

На фиг. 8 представлена система 30 обеспечения безопасности, используемая защищенной системой 20, для проверки пользователей 60, которые входят в систему через Интернет 90, например, используя модем 96.

Этап 1: Удаленный пользователь осуществляет доступ к порталу регистрации защищенной системы - только по запросу для предоставления ID пользователя, который может представлять собой адрес электронной почты, согласно ссылочным позициям 82 и 84 на фиг. 7B.

Этап 2: Пользователь вводит ID пользователя, как показано под ссылочной позицией 84 на фиг. 7B.

Этап 3: Защищенная система отправляет ID пользователя и ID системы в систему 30 обеспечения безопасности, которая выполняет проверку подлинности и возвращает матрицу 31 обеспечения безопасности, которая затем отображается защищенной системой 20 обеспечения безопасности пользователю 60.

Этап 4: Пользователь вводит одноразовый код и входит в систему как нормальный пользователь (86

на фиг. 7B). Защищенная система 20 отправляет одноразовый код 12, ID пользователя и ID системы в систему 30 обеспечения безопасности, которая проверяет упомянутый код и предоставляет защищенной системе 20 ID сеанса, если упомянутый код прошел проверку подлинности.

На фиг. 9 система 30 обеспечения безопасности, используемая защищенной системой 20 для проверки пользователей 60, которые входят в систему через Интернет 90. В этой конфигурации одна система 30 обеспечения безопасности может обслуживать множество защищенных систем 20, что дает возможность пользователям 60 иметь одно ключевое слово для всех зарегистрированных систем. Как указывалось ранее, удаленные пользователи 60 подсоединяются к Интернету 90 через модем 96.

Этап 1: Удаленный пользователь 60 осуществляет доступ к порталу входа в защищенную системы - только по запросу для предоставления ID пользователя, который может представлять собой адрес электронной почты, согласно ссылочным позициям 82 и 84 на фиг. 7B.

Этап 2: Пользователь 60 вводит ID пользователя, как показано под ссылочной позицией 84 на фиг. 7B.

Этап 3: Защищенная система 20 отправляет ID пользователя и ID системы в систему 30 обеспечения безопасности, которая выполняет проверку подлинности и возвращает матрицу 31 обеспечения безопасности, которая затем отображается защищенной системой 20 пользователю 60.

Этап 4: Пользователь 60 вводит одноразовый код 12 и регистрируется как нормальный пользователь. Защищенная система 20 отправляет одноразовый код 12, ID пользователя и ID системы в систему 30 обеспечения безопасности, которая проверяет упомянутый код и предоставляет защищенной системе 20 ID сеанса, если упомянутый код прошел проверку подлинности.

На фиг. 10 представлена внутренняя система 30 обеспечения безопасности, сконфигурированная для обслуживания финансового учреждения по всем его финансовым делам, и которая эффективно заменяет стандартные системы аутентификации, такие как системы, основанные на паролях и PIN-кодах, для дебитных и кредитных систем, используемых в расчетных узлах, банковских автоматах (ATM), в оптовой или Интернет-торговле. В приведенном выше примере показаны:

(a) Интернет-банкинг через сеть Интернет

(b) Другие Интернет-услуги, такие как обмен акциями или обмен иностранной валюты

(c) Банковские автоматы

(d) Точки продаж

(e) Персональный компьютер для обслуживания клиентов

(f) Офисные персональные компьютеры.

Ниже описываются системы, показанные на фиг. 10.

Интернет-банкинг через сеть Интернет

Если пользователь входит в Интернет-портал 90 банка обычным порядком, то в процессе вхождения запрашивается только ID пользователя (смотри ссылочные позиции 82, 84 на фиг. 7B). После приема ID пользователя компьютер 20 банка связывается с системой 30 обеспечения безопасности, сообщая ID пользователя и ID банковской системы. После проверки подлинности ID пользователя и ID системы система 30 обеспечения безопасности создает матрицу безопасности и передает ее обратно на компьютер 20 банка, после чего отображает эту матрицу пользователю 110 вместе с запросом на ввод одноразового кода, как это показано под ссылочной позицией 86 на фиг. 7B. Используя матрицу обеспечения безопасности, пользователь создает одноразовый код и вводит его в систему. Этот одноразовый код поступает обратно в компьютер 20 банка, который затем направляет этот одноразовый код, ID пользователя и ID банковской системы обратно в систему 30 обеспечения безопасности, где проверяется подлинность одноразового кода. Если его подлинность подтверждается, то создается ID сеанса, который передается обратно на компьютер 20 банка, а затем возвращается обратно в Интернет-приложение 110 для формирования части всех последующих запросов, создаваемых для компьютера 20 банка.

Другие Интернет-услуги, такие как обмен акциями или обмен иностранной валюты

Пользователь входит на Интернет-портале банка в качестве нормального пользователя, причем в процессе входа запрашивается только ID пользователя (согласно 82, 84 на фиг. 7B). После приема ID пользователя компьютер 20 банка связывается с системой 30 обеспечения безопасности, передавая ID пользователя и ID банковской системы. После проверки подлинности ID пользователя и ID системы система 30 обеспечения безопасности создает матрицу обеспечения безопасности и направляет ее обратно на компьютер 20 банка, который отображает эту матрицу пользователю 112 вместе с запросом на ввод одноразового кода. Используя матрицу обеспечения безопасности, пользователь 112 создает одноразовый код и вводит его в систему. Этот одноразовый код поступает обратно в компьютер 20 банка, который затем направляет этот одноразовый код, ID пользователя и ID банковской системы обратно в систему 30 обеспечения безопасности, где проверяется подлинность одноразового кода. Если его подлинность подтверждается, то создается ID сеанса, который передается обратно на компьютер 20 банка, а затем возвращается обратно в Интернет-приложение 112 для формирования части всех последующих запросов, создаваемых для компьютера 20 банка.

Банковские автоматы (ATM)

Пользователь, как обычно, вводит карту ATM или кредитную карту в ATM 102a, 102b банка, после

чего АТМ передает ID пользователя и любую другую соответствующую информацию на компьютер 20 банка через сеть 116 банковских автоматов. Затем компьютер 20 банка связывается с системой 30 обеспечения безопасности, передавая ID пользователя и ID банковской системы. После подтверждения подлинности ID пользователя и ID системы система 30 обеспечения безопасности создает матрицу обеспечения безопасности и направляет ее обратно на компьютер 20 банка, который возвращает эту матрицу на АТМ 102a, 102b для ее отображения пользователю. Используя матрицу обеспечения безопасности, пользователь 102a, 102b создает одноразовый код и вводит его с клавиатуры АТМ. Этот одноразовый код поступает через сеть 116 банковских автоматов обратно в компьютер 20 банка, который затем направляет этот одноразовый код, ID пользователя и ID банковской системы обратно в систему 30 обеспечения безопасности, где проверяется подлинность одноразового кода. Если его подлинность подтверждается, то создается ID сеанса, который передается обратно на компьютер 20 банка для формирования части всех последующих запросов, создаваемых для компьютера 20 банка.

Точка продаж

Пользователь вводит/прокатывает карту АТМ или кредитную карту через устройство 104 точки продаж фирмы-поставщика, после чего в обычном порядке вводится цена, а затем через сеть 114 банковских карт в компьютер 20 банка посылается соответствующая информация. Затем компьютер 20 банка связывается с системой 30 обеспечения безопасности, сообщая ID пользователя и ID банковской системы. После проверки подлинности ID пользователя и ID системы, система 30 обеспечения безопасности создает матрицу обеспечения безопасности и отправляет ее обратно на компьютер 20 банка, который возвращает ее в устройство 104 точки продаж для отображения на экране, если это возможно, или для распечатки бумажного чека. Используя матрицу обеспечения безопасности, пользователь создает одноразовый код и вводит его с клавиатуры 104 точки продаж. Этот одноразовый код направляется на компьютер 20 банка, который переправляет этот одноразовый код, ID пользователя и ID банковской системы обратно в систему 30 обеспечения безопасности, где этот одноразовый код проверяется. Если подтверждается его правильность, создается ID сеанса, который направляется обратно в банковскую систему 20, где обрабатывается остальная часть транзакции обычным образом.

Персональный компьютер для обслуживания клиентов

Попав в точку обслуживания клиентов в отделении банка, пользователь выполняет самоидентификацию, используя карты банкинга или любой другой способ корректной идентификации, который дает возможность сотруднику по работе с клиентами идентифицировать ID пользователя, и ввести его в портал 108 обслуживания клиентов. Персональный компьютер 108 для обслуживания клиентов отправляет ID пользователя в компьютер 20 банка. Далее компьютер 20 банка связывается с системой 30 обеспечения безопасности, используя ID пользователя и ID банковской системы. После проверки правильности ID пользователя и ID системы, система 30 обеспечения безопасности создает матрицу обеспечения безопасности и отправляет ее обратно на компьютер 20 банка, который возвращает ее на персональный компьютер 108 для обслуживания клиентов для отображения ее пользователю. Используя предусмотренное устройство ввода, пользователь создает одноразовый код и вводит его в персональный компьютер 108 для обслуживания клиентов. Этот одноразовый код направляется на компьютер 20 банка, который переправляет этот одноразовый код, ID пользователя и ID банковской системы обратно в систему 30 обеспечения безопасности, где этот одноразовый код проверяется. Если подтверждается его правильность, создается ID сеанса, который направляется обратно в банковскую систему 20, а затем на персональный компьютер 108 для обслуживания клиентов для формирования части всех последующих запросов, выполняемых для компьютера банка.

Офисные персональные компьютеры

Пользователь входит в корпоративную сеть посредством регистрации через нормальный портал 106; причем в процессе входа запрашивается для предъявления только ID пользователя. После предъявления ID пользователя компьютер банка связывается с системой 30 обеспечения безопасности, используя ID пользователя и ID банковской системы. После проверки подлинности ID пользователя и ID системы, система 30 обеспечения безопасности создает матрицу обеспечения безопасности и отправляет ее обратно на компьютер 20 банка, который отображает ее пользователю вместе с запросом на ввод одноразового кода. Используя матрицу обеспечения безопасности, пользователь создает одноразовый код и вводит его в систему 106 офисных персональных компьютеров. Этот одноразовый код направляется на компьютер 20 банка, который переправляет этот одноразовый код, ID пользователя и ID банковской системы обратно в систему 30 обеспечения безопасности, где этот одноразовый код проверяется. Если подтверждается его правильность, создается ID сеанса, который направляется обратно в компьютер 20 банка, который переправляет его на офисный персональный компьютер 106 для формирования части всех последующих запросов, адресованных компьютеру 20 банка.

Поддержка пользователя в панической ситуации

В одном усовершенствованном варианте система обеспечения безопасности кроме того позволяет поддержать пользователя в панической ситуации. В этом варианте пользователь или владелец системы использует конкретное префиксное число или альтернативное ключевое слово вместо нормального ключевого слова для формирования одноразового кода из матрицы обеспечения безопасности. Когда система

30 обеспечения безопасности проверяет одноразовый код и определяет, что было использовано альтернативное ключевое слово, она запускает предупредительный сигнал о панической ситуации, который поступает в защищенную систему 20. Это дает возможность защищенной системе 20 отреагировать таким образом, чтобы защитить клиента, находящегося в состоянии стресса, например, показывая ему существенно заниженный баланс для Интернет- или АТМ-систем 102a, 102b или, учитывая необходимость защиты клиента, обеспечивая безопасный доступ в бизнес-систему (на основе технологии "sandbox" (песочница)).

На фиг. 11 представлены описания структуры сообщений. Этими сообщениями являются сообщение 11 с запросом аутентификации, сообщение 12 с одноразовым кодом, сообщение 31 с матрицей обеспечения безопасности, сообщение 32 с результатом аутентификации и сообщение 33 о выполнении. Сообщение 11 с запросом аутентификации включает в себя уникальный ID пользователя и в некоторых вариантах обеспечения безопасности идентификатор (ID) системы, запрашивающей аутентификацию. Сообщение с одноразовым кодом включает в себя уникальный ID пользователя и в некоторых вариантах ID системы, запрашивающей аутентификацию, а также одноразовый код, введенный пользователем. Сообщение 31 с матрицей обеспечения безопасности включает в себя набор пар "ключ-значение", составленный в соответствии с предпочтениями 50 защищенной системы. Сообщение 32 с результатом аутентификации включает в себя в некоторых вариантах осуществления изобретения ID сеанса, индикацию о выполнении или индикацию об ошибке. Сообщение 33 о выполнении включает в себя уникальный ID пользователя и в некоторых вариантах осуществления изобретения - проверенный ID системы и ID сеанса.

На фиг. 12 показаны пользовательские предпочтения. Пользовательские предпочтения включают в себя параметр порядка, параметр сдвига, параметр обхода, параметр скачка, параметр маски и рандомизатор. В соответствии с параметром порядка линейная абстракция означает, что матрица содержит буквы ключей, представленные в линейном порядке от A до Z и от 0 до 9. Случайная абстракция означает, что матрица содержит буквы ключей, представленные в случайном порядке.

Параметр сдвига задает либо положительный, либо отрицательный сдвиг. При положительном сдвиге к каждому значению, связанному с ключом, добавляется положительная величина. Суммирование выполняется по модулю 10, а для символов - по модулю 26, так что Z+1=A. При использовании отрицательного сдвига к каждому значению, связанному с ключом, добавляется отрицательная величина. Суммирование выполняется по модулю 10 для чисел и по модулю 26 для символов.

Параметр обхода задает либо положительное, либо отрицательное приращение. Положительное приращение означает, что к значению, связанному с ключом, добавляется заданная положительная величина, а затем она возрастает на заданную величину при следующем добавлении. Отрицательное приращение означает, что к значению, связанному с ключом, добавляется заданная отрицательная величина, а затем она возрастает на заданную величину при следующем добавлении. Опять же суммирование выполняется по модулю 10 для чисел и по модулю 26 для символов.

Параметр скачка задает либо четное, либо нечетное значение для скачка. Если для этого параметра задано нечетное значение (Odd), то к каждому значению, связанному с ключом, добавляется заданная величина скачка при нечетном индексе ключевого слова, и эта величина вычитается из каждого значения в случае четного индекса ключевого слова. Если для параметра скачка задано четное значение (Even), то упомянутая заданная величина вычитается из каждого значения, связанного с ключом, при нечетном индексе ключевого слова, и заданная величина добавляется к каждому значению при четном индексе ключевого слова. Суммирование или вычитание выполняется по модулю 10 для чисел и по модулю 26 для символов.

Параметр маски определяет, что заданный символ в одном или более индексах в ключевом слове не должен изменяться на другой параметр. Дополнительно, метка (#) кэширования на том или ином месте в ключевом слове представляет подстановочный символ, на место которого пользователь может ввести любое число или любой символ.

Рандомизатор может представлять собой букву или слово, содержащее такое же количество символов, что и ключевое слово. Если рандомизатор представлен одной буквой, то его числовое значение из матрицы суммируется по модулю 10 с каждым числовым значением ключевого слова. Если рандомизатор представлен словом, то тогда значение каждой буквы в рандомизаторе-слове суммируется по модулю 10 с соответствующей буквой в ключевом слове.

На фиг. 13 показаны предпочтения защищенной системы. Эти предпочтения задают формат возврата, область определения ключа и область определения значения. Формат возврата может представлять собой формат XML, HTML, изображение или текст CSV. Область определения ключа определяет, что системе обеспечения безопасности следует формировать ключи матрицы обеспечения безопасности с использованием заданных символов. Область определения значения определяет, что защищенной системе следует формировать значения матрицы обеспечения безопасности с использованием заданных символов.

На фиг. 14 представлена блок-схема варианта осуществления настоящего изобретения. Эта блок-схема описывает этапы, которые выполняют клиентский интерфейс, защищенная система и система обеспечения безопасности для аутентификации пользователя, запрашивающего доступ в защищенную

систему. На этапе 150 пользователь предоставляет системе обеспечения безопасности ключевое слово и свои предпочтения, а система обеспечения безопасности на этапе 152 принимает эти позиции и сохраняет их в устройстве постоянного хранения.

На этапе 154 пользователь запрашивает авторизацию на клиентском интерфейсе, который на этапе 156 отправляет этот запрос в защищенную систему. На этапе 158 защищенная система принимает этот запрос аутентификации и направляет его вместе с ID системы в систему обеспечения безопасности, которая принимает этот запрос аутентификации на этапе 160. Затем система обеспечения безопасности на этапе 162 создает матрицу обеспечения безопасности и отправляет эту матрицу в защищенную систему на этапе 164a или 164b. На этапе 164a защищенная система направляет эту матрицу на клиентский интерфейс, который ее принимает на этапе 166. На этапе 164b защищенная система осуществляет построение пользовательского представления матрицы обеспечения безопасности и отправляет его на клиентский интерфейс, который принимает эту матрицу на этапе 166.

На этапе 166 пользователь также создает одноразовый код, используя матрицу обеспечения безопасности, свое ключевое слово и свои предпочтения и вводит этот одноразовый код в клиентский интерфейс на этапе 168. Затем клиентский интерфейс посылает указанный одноразовый код в защищенную систему на этапе 170, которая принимает указанный одноразовый код на этапе 172 и направляет его вместе с ID пользователя и ID системы в систему обеспечения безопасности, которая принимает указанное на этапе 174. На этом этапе система обеспечения безопасности проверяет указанный одноразовый код, используя матрицу обеспечения безопасности, посланную ранее, пользовательское ключевое слово и пользовательские предпочтения. На этапе 176 система обеспечения безопасности посылает результаты аутентификации в защищенную систему вместе с ID сеанса, если результат аутентификации был успешен. На этапе 178 защищенная система направляет этот результат на клиентский интерфейс. Отдельно, на этапе 182 система обеспечения безопасности посылает сообщение о выполнении или невыполнении аутентификации в систему обеспечения безопасности, которая принимает указанное сообщение на этапе 184.

На фиг. 15 показана блок-схема варианта осуществления изобретения для создания и отправки одноразового кода. На этапе 190 матрица обеспечения безопасности отображается на клиентском интерфейсе. Эта матрица может быть представлена в алфавитном порядке или в случайном порядке в зависимости от того, какой порядок задан в пользовательских предпочтениях. На этапе 192 пользователь создает одноразовый код, используя упомянутое ключевое слово, матрицу обеспечения безопасности и пользовательские предпочтения, которые определяют, следует ли использовать сдвиги, обходы, скачки и маски либо любую их комбинацию для формирования одноразового кода. На этапе 194 пользователь вводит этот одноразовый код в клиентский интерфейс, с тем чтобы его можно было переслать в защищенную систему.

В первом аспекте настоящего изобретения обеспечен способ аутентификации пользователя, содержащий исполнение системой (30) обработки следующих этапов, на которых: принимают (160) запрос (11) от пользователя (10) для инициирования сеанса аутентификации, причем запрос (11) содержит уникальный идентификатор пользователя (10); осуществляют доступ с использованием уникального идентификатора, к записи, сохраненной в памяти, связанной с пользователем, причем сохраненная запись содержит, по меньшей мере, данные (40) о сложности преобразования последовательности кодовых значений, которые определяют предпочитаемый пользователем уровень сложности для использования при проверке пользовательского ввода, принимаемого в ответ на представление матриц (31) обеспечения безопасности, и определенное пользователем ключевое слово (41), состоящее из упорядоченной последовательности символов, содержащей элементы заранее определенного набора символов, выбранного из одного или более наборов символов, поддерживаемых системой (30) обработки, при этом символы упорядоченной последовательности были ранее выбраны пользователем (10) независимо от выборов других пользователей; создают (162) матрицу (31) обеспечения безопасности, которая является действительной для упомянутого пользователя (10) только во время данного сеанса аутентификации и которая содержит соответствие между каждым символом из упомянутого заранее определенного набора символов и каждым кодовым значением (12) из кодового набора, который отличается от упомянутого заранее определенного набора символов и который формируется для матрицы (31) обеспечения безопасности случайным образом для каждого сеанса аутентификации; передают (164a) матрицу (31) обеспечения безопасности для представления (190) пользователю (10); принимают (172) упорядоченную последовательность кодовых значений (12), выбранных пользователем (10) из матрицы (31) обеспечения безопасности и введенных (194) пользователем (10) на основе определенного пользователем ключевого слова (41) и данных (40) о сложности преобразования последовательности кодовых значений, в ответ на представление (190) матрицы (31) обеспечения безопасности; проверяют (174) принятую упорядоченную последовательность кодовых значений путем сравнения с соответствующей последовательностью кодовых значений, созданной, но не переданной системой (30) обработки, на основе определенного пользователем ключевого слова (41) в сохраненной записи, данных (40) о сложности преобразования последовательности кодовых значений и матрицы (31) обеспечения безопасности; и создают (178) результат (32) аутентификации сеанса аутентификации на основе упомянутого сравнения.

В упомянутом способе этап создания матрицы обеспечения безопасности содержит упорядочение символов в упомянутом заранее определенном наборе символов в случайном порядке.

В упомянутом способе этап создания матрицы обеспечения безопасности содержит упорядочение символов в упомянутом заранее определенном наборе символов в алфавитном порядке.

В упомянутом способе этап приема запроса от пользователя содержит прием запроса от защищенной системы, отличной от упомянутой системы обработки, причем упомянутая защищенная система имеет соответствующий идентификатор защищенной системы; причем запрос дополнительно содержит идентификатор защищенной системы; и этап создания матрицы обеспечения безопасности основан на предпочтениях защищенной системы, связанных с идентификатором защищенной системы, при этом предпочтения защищенной системы определяют одно или более из формата возвращаемых данных защищенной системы, области определения набора символов, и области определения кодового набора.

В упомянутом способе этап передачи матрицы обеспечения безопасности для представления пользователю содержит: передачу матрицы обеспечения безопасности в защищенную систему; построение защищенной системой пользовательского представления матрицы обеспечения безопасности; и представление защищенной системой пользователю пользовательского представления матрицы обеспечения безопасности.

В упомянутом способе этап создания матрицы обеспечения безопасности включает в себя случайный выбор кодовых значений из кодового набора, определенного в соответствии с предпочтениями защищенной системы, связанными с идентификатором защищенной системы.

В упомянутом способе заранее определенный набор символов содержит алфавитные символы, и в котором кодовый набор представляет собой набор числовых значений.

В упомянутом способе данные о сложности преобразования последовательности кодовых значений содержат значение сдвига, определенное так, что этап проверки принятой упорядоченной последовательности кодовых значений содержит создание соответствующей последовательности кодовых значений на основе определенного пользователем ключевого слова в упомянутой сохраненной записи, матрицы обеспечения безопасности, определяющей соответствия между символами и числовыми значениями кодового набора, и вычисление преобразованных кодовых значений на основе упомянутого значения сдвига.

В упомянутом способе данные о сложности преобразования последовательности кодовых значений содержат значение обхода, определенное так, что этап проверки принятой упорядоченной последовательности кодовых значений содержит создание соответствующей последовательности кодовых значений на основе определенного пользователем ключевого слова в упомянутой сохраненной записи, матрицы обеспечения безопасности, определяющей соответствия между символами и числовыми значениями кодового набора, и вычисление преобразованных кодовых значений на основе упомянутого значения обхода.

В упомянутом способе данные о сложности преобразования последовательности кодовых значений содержат значение скачка, определенное так, что этап проверки принятой упорядоченной последовательности кодовых значений содержит создание соответствующей последовательности кодовых значений на основе определенного пользователем ключевого слова в упомянутой сохраненной записи, матрицы обеспечения безопасности, определяющей соответствия между символами и числовыми значениями кодового набора, и вычисление преобразованных кодовых значений на основе упомянутого значения скачка.

В упомянутом способе данные о сложности преобразования последовательности кодовых значений содержат значение маски, определенное так, что этап проверки принятой упорядоченной последовательности кодовых значений содержит создание соответствующей последовательности кодовых значений на основе определенного пользователем ключевого слова в упомянутой сохраненной записи, матрицы обеспечения безопасности, определяющей соответствия между символами и числовыми значениями кодового набора, и вычисление преобразованных кодовых значений на основе упомянутого значения маски.

В упомянутом способе сохраненная запись, связанная с пользователем, содержит альтернативное определенное пользователем ключевое слово, состоящее из упорядоченной последовательности символов, выбранных из заранее определенного набора символов, и в котором этап проверки принятой упорядоченной последовательности кодовых значений дополнительно содержит выполнение сравнения с соответствующей последовательностью кодовых значений, созданной, но не переданной системой обработки на основе альтернативного определенного пользователем ключевого слова в сохраненной записи, данных о сложности преобразования последовательности кодовых значений, и матрицы обеспечения безопасности; и в случае, когда упомянутое сравнение приводит в результате к совпадению, создание результата аутентификации упомянутого сеанса аутентификации, содержащего указание о панической ситуации.

Во втором аспекте настоящего изобретения обеспечено устройство (30) аутентификации пользователя, содержащее хранилище данных; и процессор, содержащий блок обработки и сохраненные программные инструкции, которые при исполнении побуждают блок обработки реализовывать способ в соответствии с вышеупомянутым первым аспектом настоящего изобретения.

В третьем аспекте настоящего изобретения обеспечена система обеспечения безопасности, содержащая устройство аутентификации пользователя в соответствии с вышеупомянутым вторым аспектом настоящего изобретения и защищенную систему (20), для которой пользователь запрашивает аутентификацию и которая сконфигурирована для приема уникального идентификатора пользователя; передачи запроса для инициирования сеанса аутентификации в устройство аутентификации пользователя, причем запрос содержит уникальный идентификатор пользователя; приема от устройства аутентификации пользователя матрицы обеспечения безопасности; представления пользователю матрицы обеспечения безопасности; приема от пользователя упорядоченной последовательности кодовых значений, выбранных из матрицы обеспечения безопасности; передачи упорядоченной последовательности кодовых значений в устройство аутентификации пользователя и приема от устройства аутентификации пользователя результата аутентификации.

В упомянутой системе защищенная система содержит одно из: интерфейса веб-сервера, при этом ввод принимается от пользователя и матрица обеспечения безопасности представляется пользователю через веб-браузер (110, 112), управляемый пользователем; банковский автомат (102a, 102b) или терминал (104) точки продаж.

Хотя настоящее изобретение было достаточно подробно описано со ссылками на конкретные предпочтительные версии его осуществления, возможны и другие версии. Таким образом, существо и объем прилагаемой формулы изобретения не следует ограничивать описанием приведенных здесь предпочтительных версий осуществления изобретения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ аутентификации пользователя, содержащий исполнение системой (30) обработки следующих этапов, на которых:

принимают (160) запрос (11) от пользователя (10) для инициирования сеанса аутентификации, причем запрос (11) содержит уникальный идентификатор пользователя (10);

осуществляют доступ с использованием уникального идентификатора к записи, сохраненной в памяти, связанной с пользователем, причем сохраненная запись содержит, по меньшей мере, данные (40) о сложности преобразования последовательности кодовых значений, которые определяют предпочитаемый пользователем уровень сложности для использования при проверке пользовательского ввода, принимаемого в ответ на представление матриц (31) обеспечения безопасности, и определенное пользователем ключевое слово (41), состоящее из упорядоченной последовательности символов, содержащей элементы заранее определенного набора символов, выбранного из одного или более наборов символов, поддерживаемых системой (30) обработки, при этом символы упорядоченной последовательности были ранее выбраны пользователем (10) независимо от выборов других пользователей;

создают (162) матрицу (31) обеспечения безопасности, которая является действительной для упомянутого пользователя (10) только во время данного сеанса аутентификации и которая содержит соответствие между каждым символом из упомянутого заранее определенного набора символов и каждым кодовым значением (12) из кодового набора, который отличается от упомянутого заранее определенного набора символов и который формируется для матрицы (31) обеспечения безопасности случайным образом для каждого сеанса аутентификации;

передают (164a) матрицу (31) обеспечения безопасности для представления (190) пользователю (10);

принимают (172) упорядоченную последовательность кодовых значений (12), выбранных пользователем (10) из матрицы (31) обеспечения безопасности и введенных (194) пользователем (10) на основе определенного пользователем ключевого слова (41) и данных (40) о сложности преобразования последовательности кодовых значений, в ответ на представление (190) матрицы (31) обеспечения безопасности;

проверяют (174) принятую упорядоченную последовательность кодовых значений путем сравнения с соответствующей последовательностью кодовых значений, созданной, но не переданной системой (30) обработки, на основе определенного пользователем ключевого слова (41) в сохраненной записи, данных (40) о сложности преобразования последовательности кодовых значений и матрицы (31) обеспечения безопасности и

создают (178) результат (32) аутентификации сеанса аутентификации на основе упомянутого сравнения.

2. Способ по п.1, в котором этап создания матрицы обеспечения безопасности содержит упорядочение символов в упомянутом заранее определенном наборе символов в случайном порядке.

3. Способ по п.1, в котором этап создания матрицы обеспечения безопасности содержит упорядочение символов в упомянутом заранее определенном наборе символов в алфавитном порядке.

4. Способ по п.1, в котором

этап приема запроса от пользователя содержит прием запроса от защищенной системы, отличной от упомянутой системы обработки, причем упомянутая защищенная система имеет соответствующий идентификатор защищенной системы;

причем запрос дополнительно содержит идентификатор защищенной системы; и

этап создания матрицы обеспечения безопасности основан на предпочтениях защищенной системы, связанных с идентификатором защищенной системы, при этом предпочтения защищенной системы определяют одно или более из формата возвращаемых данных защищенной системы, области определения набора символов и области определения кодового набора.

5. Способ по п.4, в котором этап передачи матрицы обеспечения безопасности для представления пользователю содержит

передачу матрицы обеспечения безопасности в защищенную систему;

построение защищенной системой пользовательского представления матрицы обеспечения безопасности и

представление защищенной системой пользователю пользовательского представления матрицы обеспечения безопасности.

6. Способ по п.4, в котором этап создания матрицы обеспечения безопасности включает в себя случайный выбор кодовых значений из кодового набора, определенного в соответствии с предпочтениями защищенной системы, связанными с идентификатором защищенной системы.

7. Способ по п.1, в котором заранее определенный набор символов содержит алфавитные символы и в котором кодовый набор представляет собой набор числовых значений.

8. Способ по п.7, в котором данные о сложности преобразования последовательности кодовых значений, содержат значение сдвига, определенное так, что этап проверки принятой упорядоченной последовательности кодовых значений содержит создание соответствующей последовательности кодовых значений на основе определенного пользователем ключевого слова в упомянутой сохраненной записи, матрицы обеспечения безопасности, определяющей соответствия между символами и числовыми значениями кодового набора, и вычисление преобразованных кодовых значений на основе упомянутого значения сдвига.

9. Способ по п.7, в котором данные о сложности преобразования последовательности кодовых значений содержат значение обхода, определенное так, что этап проверки принятой упорядоченной последовательности кодовых значений содержит создание соответствующей последовательности кодовых значений на основе определенного пользователем ключевого слова в упомянутой сохраненной записи, матрицы обеспечения безопасности, определяющей соответствия между символами и числовыми значениями кодового набора, и вычисление преобразованных кодовых значений на основе упомянутого значения обхода.

10. Способ по п.7, в котором данные о сложности преобразования последовательности кодовых значений содержат значение скачка, определенное так, что этап проверки принятой упорядоченной последовательности кодовых значений содержит создание соответствующей последовательности кодовых значений на основе определенного пользователем ключевого слова в упомянутой сохраненной записи, матрицы обеспечения безопасности, определяющей соответствия между символами и числовыми значениями кодового набора, и вычисление преобразованных кодовых значений на основе упомянутого значения скачка.

11. Способ по п.7, в котором данные о сложности преобразования последовательности кодовых значений содержат значение маски, определенное так, что этап проверки принятой упорядоченной последовательности кодовых значений содержит создание соответствующей последовательности кодовых значений на основе определенного пользователем ключевого слова в упомянутой сохраненной записи, матрицы обеспечения безопасности, определяющей соответствия между символами и числовыми значениями кодового набора, и вычисление преобразованных кодовых значений на основе упомянутого значения маски.

12. Способ по п.7, в котором сохраненная запись, связанная с пользователем, содержит альтернативное определенное пользователем ключевое слово, состоящее из упорядоченной последовательности символов, выбранных из заранее определенного набора символов, и в котором

этап проверки принятой упорядоченной последовательности кодовых значений дополнительно содержит выполнение сравнения с соответствующей последовательностью кодовых значений, созданной, но не переданной системой обработки на основе альтернативного определенного пользователем ключевого слова в сохраненной записи, данных о сложности преобразования последовательности кодовых значений и матрицы обеспечения безопасности; и

в случае, когда упомянутое сравнение приводит в результате к совпадению, создание результата аутентификации упомянутого сеанса аутентификации, содержащего указание о панической ситуации.

13. Устройство (30) аутентификации пользователя, содержащее хранилище данных и процессор, содержащий блок обработки и сохраненные программные инструкции, которые при исполнении побуждают блок обработки реализовывать способ по п.1.

14. Система обеспечения безопасности, содержащая

устройство аутентификации пользователя по п.13 и защищенную систему (20), для которой пользователь запрашивает аутентификацию, и которая сконфигурирована для

приема уникального идентификатора пользователя;

передачи запроса для инициирования сеанса аутентификации в устройство аутентификации пользователя, причем запрос содержит уникальный идентификатор пользователя;

приема от устройства аутентификации пользователя матрицы обеспечения безопасности;

представления пользователю матрицы обеспечения безопасности;

приема от пользователя упорядоченной последовательности кодовых значений, выбранных из матрицы обеспечения безопасности;

передачи упорядоченной последовательности кодовых значений в устройство аутентификации пользователя и

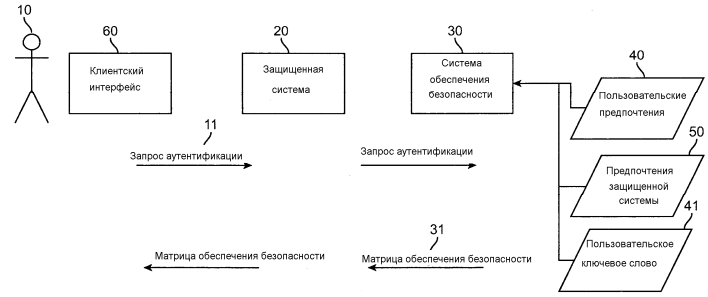
приема от устройства аутентификации пользователя результата аутентификации.

15. Система обеспечения безопасности по п.14, в которой защищенная система содержит одно из:

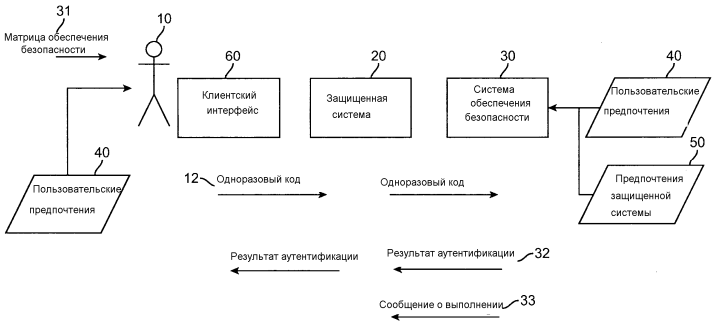
интерфейс веб-сервера, при этом ввод принимается от пользователя и матрица обеспечения безопасности представляется пользователю через веб-браузер (110, 112), управляемый пользователем;

банковский автомат (102a, 102b) или

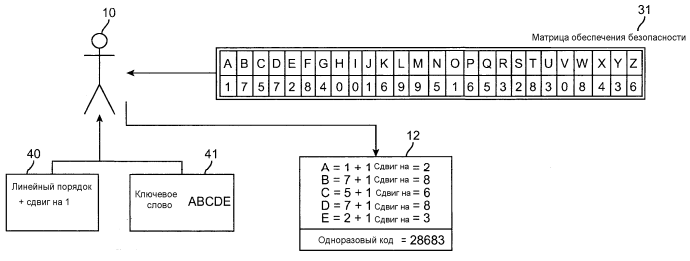
терминал (104) точки продаж.



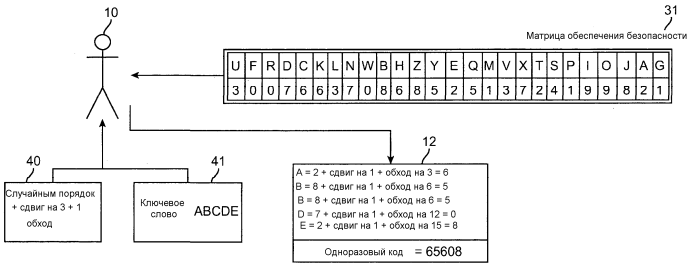
Фиг. 1



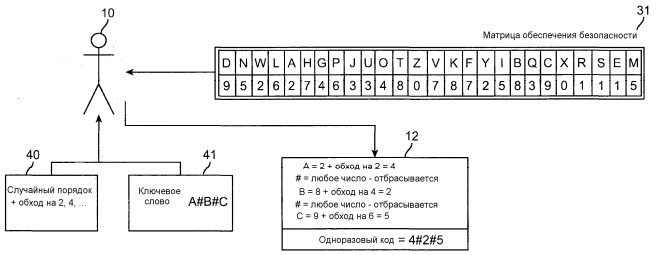
Фиг. 2



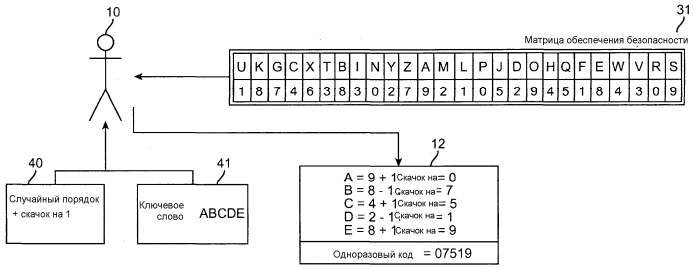
Фиг. 3



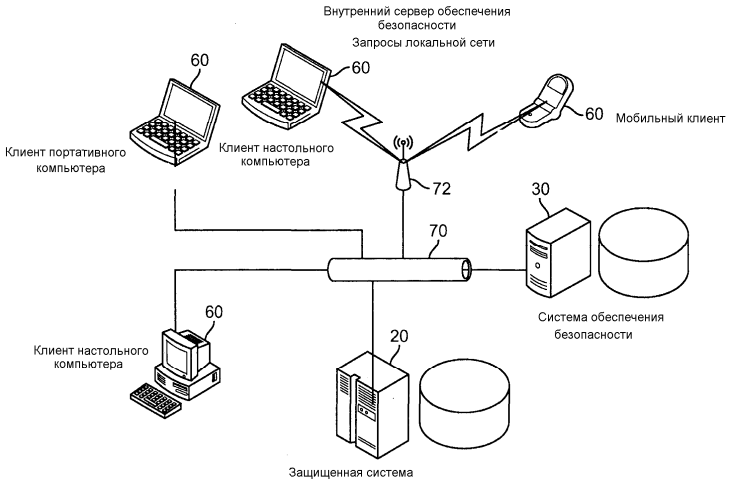
Фиг. 4



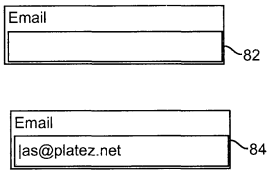
Фиг. 5

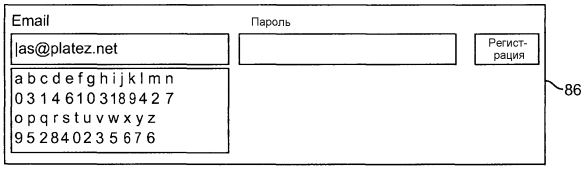


Фиг. 6

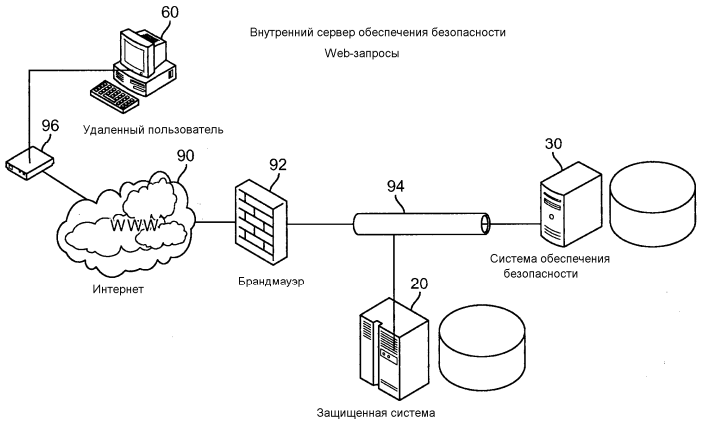


Фиг. 7A

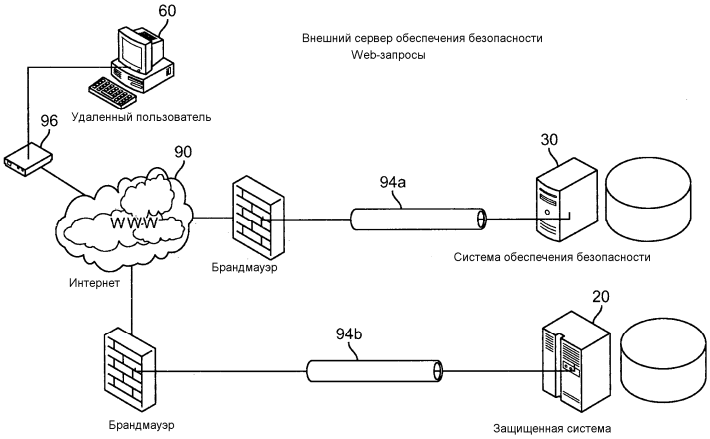




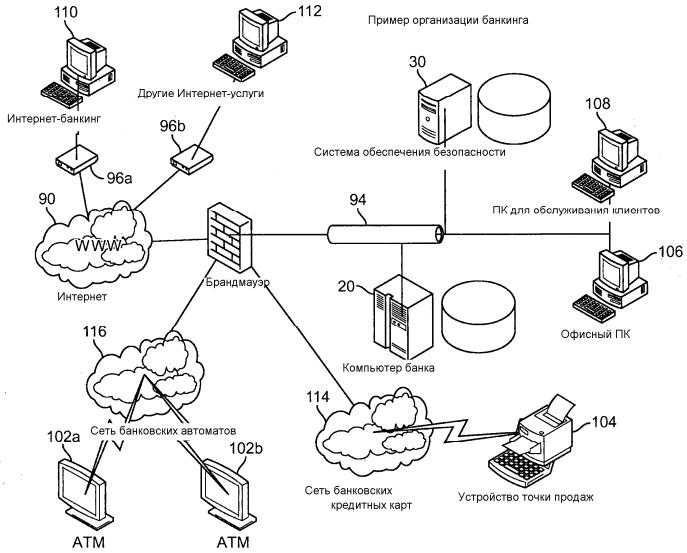
Фиг. 7B



Фиг. 8



Фиг. 9



Фиг. 10

Таблица 1

Запрос 11 аутентификации Уникальный ID пользователя ID системы, запрашивающей аутентификацию Одноразовый код 12 ID системы, запрашивающей проверку Одноразовый код, введенный конечным пользователем Матрица 31 обеспечения безопасности Набор пар ключ/значение, составленных в соответствии с предпоч-тениями 50 защищенной системы Результат 32 аутентификации ID сеанса, OK или Ошибка Сообщение 33 о выполнении Уникальный ID пользователя ID системы, подвергнутой проверке ID сеанса

Фиг. 11

Таблица 3

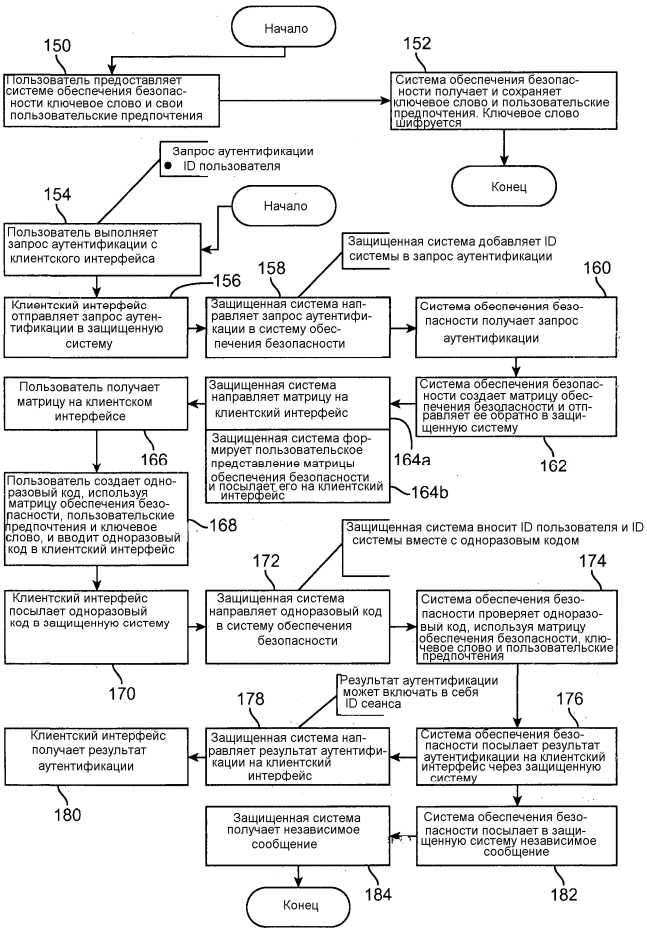
Сегмент	Опция	Описание
Порядок	Линейная абстракция	Буквы ключа, представленные в линейном порядке от A до Z, от 0 до 9
Порядок	Случайная абстракция	Буквы ключа, представленные в случайном порядке
Сдвиг	Положительный сдвиг	Величина, добавляемая к каждому значению, связанному с ключом. Выполняется свертка чисел, например, 9+1=0, а также свертка букв, например, Z+1=A, то есть +1
Сдвиг	Отрицательный сдвиг	Величина, вычитаемая из каждого значения связанного с ключом. Выполняется свертка чисел, например, 0-1=9, а также свертка букв, например, A-1=Z, то есть -1
Обход	Отрицательное приращение	Отрицательное приращение
Обход	Отрицательное приращение	Величина, вычитаемая из каждого значения связанного с ключом, с последующим отрицательным приращением. Выполняется свертка чисел, например, 0-1=9, а также свертка букв, например, A-1=Z, то есть -2 (инициирование последовательности 0,-2,-4,-6,-8, вычитаемой с приращением)
Скачок	Нечетный	Эта величина добавляется к каждому значению, расположенному с нечетным индексом ключевого слова, и вычитается из каждого значения, расположенного с четным индексом ключевого слова
Скачок	Четный	Эта величина вычитается из каждого значения, расположенного с нечетным индексом ключевого слова, и добавляется к каждому значению, расположенному с четным индексом ключевого слова
Маска	Согласно определению	*Маска является расширением шаблона ключевого слова*, так что *символ-заполнитель определяется* с некоторыми индексами ключевого слова. Символом-заполнителем может быть любое число/буква/символ, который не применяется для какой-либо другой опции. Дополнительно, символ # представляет подстановочный знак, позволяя пользователю задать ключевое слово, которое выглядит длиннее, чем на самом деле
Рандоми-затор	Единый	Пользователь выбирает единый ключ из области определения ключа, чье значение используется затем для модификации каждого отдельного значения в ключевом слове. Например, FRED=6152 является ключевым словом, P=3 является единым ключом, выбранным рандомизатором, так что получается одноразовый код 9485 в предположении, что никакой другой модификатор не применялся
Рандоми-затор	Ключ	Пользователь выбирает второй полный ключ такой же длины, как ключевое слово; каждый маркер в этом рандомизированном ключе используется для модификации каждого соответствующего значения в ключевом слове. Например, FRED=6152 является ключевым словом, JOHN=1493 является ключом рандомизатора, так что получается одноразовый код 7545 в предположении, что никакой другой модификатор не применялся

Фиг. 12

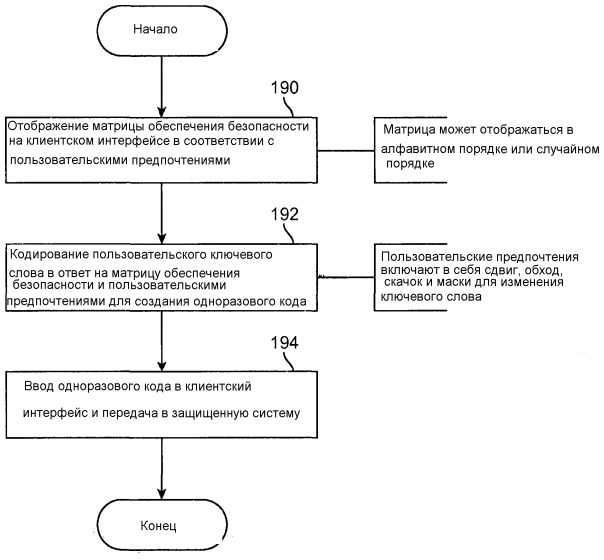
Таблица 4

Сегмент	Опция	Описание
Формат возврата	XML	Матрица обеспечения безопасности возвращается в виде структуры XML
Формат возврата	HTML	Матрица обеспечения безопасности возвращается в виде переформатированного вложения HTML
Формат возврата	Изображение	Матрица обеспечения безопасности возвращается в виде изображения
Формат возврата	CSV	Матрица обеспечения безопасности возвращается в виде читаемого текста, разделенного запятыми
Область определения ключа	Набор символов от A до Z, от a до z, от 0 до 9 или изображений	Система обеспечения безопасности формирует ключи матрицы обеспечения безопасности, используя указанные возможности отбора информации. Эта информация также определяет состав ключевого слова
Область определения значения	Набор символов от A до Z, от a до z, от 0 до 9 или изображений	Система обеспечения безопасности формирует значения матрицы обеспечения безопасности, используя указанные возможности отбора информации

Фиг. 13


Начало
150
Пользователь предоставляет системе обеспечения безопасности ключевое слово и свои пользовательские предпочтения
152
Система обеспечения безопасности получает и сохраняет ключевое слово и пользовательские предпочтения. Ключевое слово шифруется
Конец
Запрос аутентификации
ID пользователя
154
Начало
Пользователь выполняет запрос аутентификации с клиентского интерфейса
Защищенная система добавляет ID системы в запрос аутентификации
156
158
160
Клиентский интерфейс отправляет запрос аутентификации в защищенную систему
Защищенная система направляет запрос аутентификации в систему обеспечения безопасности
Система обеспечения безопасности получает запрос аутентификации
Пользователь получает матрицу на клиентском интерфейсе
Защищенная система направляет матрицу на клиентский интерфейс
Система обеспечения безопасности создает матрицу обеспечения безопасности и отправляет ее обратно в защищенную систему
Защищенная система формирует пользовательское представление матрицы обеспечения безопасности и посылает его на клиентский интерфейс
164a
162
166
164b
Пользователь создает одноразовый код, используя матрицу обеспечения безопасности, пользовательские предпочтения и ключевое слово, и вводит одноразовый код в клиентский интерфейс
168
Защищенная система вносит ID пользователя и ID системы вместе с одноразовым кодом
172
174
Клиентский интерфейс посылает одноразовый код в защищенную систему
Защищенная система направляет одноразовый код в систему обеспечения безопасности
Система обеспечения безопасности проверяет одноразовый код, используя матрицу обеспечения безопасности, ключевое слово и пользовательские предпочтения
170
Результат аутентификации может включать в себя ID сеанса
178
176
Клиентский интерфейс получает результат аутентификации
Защищенная система направляет результат аутентификации на клиентский интерфейс
Система обеспечения безопасности посылает результат аутентификации на клиентский интерфейс через защищенную систему
180
Защищенная система получает независимое сообщение
Система обеспечения безопасности посылает в защищенную систему независимое сообщение
184
182
Конец

Фиг. 14


Начало
190
Отображение матрицы обеспечения безопасности на клиентском интерфейсе в соответствии с пользовательскими предпочтениями
Матрица может отображаться в алфавитном порядке или случайном порядке
192
Кодирование пользовательского ключевого слова в ответ на матрицу обеспечения безопасности и пользовательскими предпочтениями для создания одноразового кода
Пользовательские предпочтения включают в себя сдвиг, обход, скачок и маски для изменения ключевого слова
194
Ввод одноразового кода в клиентский интерфейс и передача в защищенную систему
Конец

Фиг. 15