(19) Евразийское патентное ведомство

(11) 046717 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2024.04.16

(21) Номер заявки
202293426

(22) Дата подачи заявки
2022.12.22

(51) Int. Cl. ***H04W 12/00*** (2021.01)
G06F 21/44 (2013.01)
G06F 17/00 (2019.01)

(54) СПОСОБ И УСТРОЙСТВО ФОРМИРОВАНИЯ СТАТИЧНОГО ИДЕНТИФИКАТОРА МОБИЛЬНЫХ УСТРОЙСТВ ПОД УПРАВЛЕНИЕМ iOS, СПОСОБ И СИСТЕМА ВЫЯВЛЕНИЯ МОШЕННИЧЕСКИХ ТРАНЗАКЦИЙ С ПОМОЩЬЮ СТАТИЧНОГО ИДЕНТИФИКАТОРА

(31) **2022130031**
(32) **2022.11.18**
(33) **RU**
(43) **2024.04.15**

(71)(73) Заявитель и патентовладелец:
ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "СБЕРБАНК РОССИИ" (ПАО СБЕРБАНК) (RU)

(72) Изобретатель:
Губанов Дмитрий Николаевич,
Широков Артём Александрович (RU)

(74) Представитель:
Герасин Б.В. (RU)

(56) CN-A-112507291
CN-A-111601304
CN-A-107908948
US-A1-2018083963

(57) Изобретение относится к области компьютерной техники, в частности к методам формирования идентификаторов устройств для их применения в области защиты информации. Техническим результатом является повышение точности идентификации мобильных устройств за счет формирования статичного идентификатора. Заявленное решение осуществляется с помощью способа формирования статичного идентификатора мобильных устройств под управлением iOS, при этом способ содержит этапы, на которых с помощью процессора мобильного устройства: устанавливают платежное приложение в операционную систему (ОС) мобильного устройства; осуществляют запуск платежного приложения и регистрацию пользователя в нем, при этом осуществляют сбор параметров мобильного устройства, включающих в себя: параметры процессора, параметры ОС, параметры модуля памяти и параметры аккумуляторной батареи; переводят каждый полученный параметр в массив бит; осуществляют конкатенирование полученного массива бит полученных параметров; выполняют хэширование сконкатенированного массива бит; формируют статичный идентификатор мобильного устройства на основании выполненного хэширования; записывают полученный статичный идентификатор в закрытую область памяти мобильного устройства; связывают полученный идентификатор с платежным приложением конкретного пользователя; передают полученный идентификатор на сервер автоматизированной системы фрод-мониторинга (АСФМ).

046717 B1

046717 B1

Область техники

Изобретение относится к области компьютерной техники, в частности к методам формирования идентификаторов устройств для их применения в области защиты информации.

Уровень техники

В настоящее время применение мобильных приложений для получения финансовых услуг является широко используемым способом взаимодействия пользователей с банками. Однако с массовым распространением получения услуг в цифровом формате возросло также и количество мошеннической активности, направленной на хищение средств пользователей, что обуславливает необходимость разработки новых средств защиты пользователей от действий мошенников.

Идентификация мобильных устройств (МУ) - это процесс формирования устойчивых признаков, благодаря которым возможно установление тождественности неизвестного устройства известному на основании совпадения признаков. Таким образом, при первичном формировании идентификаторов МУ происходит генерация уникальных значений устройств, уникальность которых гарантируется алгоритмом генерирования идентификаторов (пространство вариантов составляет 2^{128}).

Современные мобильные устройства (смартфоны) представляют собой высокопроизводительные многофункциональные устройства с полноценным пользовательским интерфейсом и множеством различных радиоинтерфейсов. Производители МУ формируют различные внутренние идентификаторы устройств (уровня ОС, интерфейсов, аппаратных компонентов), доступ к которым невозможно получить на уровне прикладного ПО, установленного на МУ, либо они не обеспечивают достаточный уровень уникальности или устойчивости.

Правила конфиденциальности Apple® несут для устанавливаемых на МУ приложений ряд серьёзных ограничений (https://support.apple.com/ru-ru/HT211970), а именно:

закрытое API и отсутствие возможности получить значимые данные об аппаратном обеспечении МУ (текущая загрузка CPU, частично GPU, частично Memory, тактовая частота и пр.);

opt in - принцип, ограничивающий получение IDFA (идентификатор приложений МУ) без явного согласия пользователя на предоставление данных конкретному приложению;

маркеры приложений - принцип, определяющий тип собираемых и обрабатываемых персональных данных мобильным приложением. Блокировка работы приложения при выявлении данных выходящих за рамки заявленной маркировки.

Исследование существующих решений идентификации МУ под управлением ОС iOS привело к выводу о наличии двух основных методов:

1) идентификация на основе Unique Device Identifier (UDID), присвоенных МУ непосредственно производителем и необходимых для регистрации в портале разработчиков Apple Developer. К решениям, использующим данный метод относятся: IFunBox и SuperUDID. Однако, основным недостатком является то, что UDID необходимо установить специальное ПО на внешнее устройство, например, компьютер, к которому необходимо подключить мобильное устройство;

2) идентификация на основе HardwareID (IDFV и IDFA), получаемых на уровне прикладного ПО. К решениям, использующим данный метод относится RSA, BiZone и другие. Данный метод также нецелесообразно использовать для идентификации МУ, так как при сбросе устройства до заводских настроек, идентификатор также же изменяется.

Так как существующие методы формирования идентификаторов не имеют достаточной степени устойчивости, либо не применимы в качестве ПРОМ решений, то было принято решение о поиске и апробации собственного метода идентификации МУ.

В результате проведенных исследований не было выявлено решения, которое бы позволяло сформировать стойкий идентификатора устройств под управлением iOS, который являлся бы устойчивым к изменению аппаратной конфигурации МУ, например, восстановленным МУ. В системе iOS для хранения и использования идентификаторов МУ используется сервис Keychain Services API (https://developer.apple.com/documentation/security/keychain_services?changes=latest_minor.), предназначенный для хранения пользовательской информации в закрытой области памяти.

Данный функционал позволяет приложениям хранить несколько бит пользовательских данных в зашифрованной базе данных, называемой Keychain. Данная база данных не ограничивается парольной информацией, в ней можно также хранить и любую другую информацию, которая представляет важность для пользователя, а также элементы, которые нужны пользователю, но о существовании которых он может и не знать. Например, криптографические ключи и сертификаты, которые управляются и используются с помощью служб сертификатов и ключей, и которые позволяют пользователю участвовать в защищенной связи и устанавливать доверительные отношения с другими пользователями и устройствами.

Злоумышленники, используя различные методики воздействия на клиентов банка, в том числе социальную инженерию, могут получить доступ к критическим данным клиентов, затем эти данные могут быть использованы для установки банковских приложений на устройстве злоумышленника с дальнейшей регистрацией его в банке. Злоумышленник после регистрации такого приложения на своем устройстве от имени клиента получает доступ к денежным средствам клиента и далее предпринимает попытки хищения этих средств.

Существуют подходы в части формирования комплексных ID устройств (патентная заявка US 20140164178 A1, 12.06.2014), при которых ID формируется на основании существующей информации о регистрационных данных пользователя различных аккаунтов, позволяя тем самым сформировать более уникальный ID для применения в целях аутентификации.

Существенной проблемой существующих подходов является ключевое использование цифровой информации и базовых аппаратных номеров мобильных устройств, например, IMEI, серийный номер и т.п. Эти данные достаточно уязвимы и не позволяет формировать на их основании статичный идентификатора, который не будет существенно изменяться при заводском сбросе устройств, его аппаратной модификации и т.п.

Сущность изобретения

Заявленное изобретение позволяет решить техническую проблему в части создания устойчивого идентификатора мобильного устройства для последующего его применения для отслеживания мошеннической активности.

Техническим результатом является повышение точности идентификации мобильных устройств, за счет формирования статичного идентификатора.

Заявленное решение осуществляется с помощью способа формирования статичного идентификатора мобильных устройств под управлением iOS, при этом способ содержит этапы, на которых с помощью процессора мобильного устройства:

устанавливают платежное приложение в операционную систему (ОС) мобильного устройства;

осуществляют запуск платежного приложения и регистрацию пользователя в нем, при этом осуществляют сбор параметров мобильного устройства, включающих в себя: параметры процессора, параметры ОС, параметры модуля памяти и параметры аккумуляторной батареи;

переводят каждый полученный параметр в массив бит;

осуществляют конкатенирование полученного массива бит полученных параметров;

выполняют хэширование сконкатенированного массива бит;

формируют статичный идентификатор мобильного устройства на основании выполненного хэширования;

записывают полученный статичный идентификатор в закрытую область памяти мобильного устройства;

связывают полученный идентификатор с платежным приложением конкретного пользователя;

передают полученный идентификатор на сервер автоматизированной системы фрод-мониторинга (АСФМ).

В одном из частных примеров реализации параметры процессора включают по меньшей мере одно из: название процессора, номинальная частота процессора, количество физических ядер, количество логических ядер, процент утилизации процессора системой, процент утилизации процессора пользователем, процент утилизации процессора в простое.

В другом частном примере реализации параметры ОС включают по меньшей мере одно из: признак запуска, код языка на устройстве, код региона на устройстве, код таймзоны на устройстве, семейство устройств, полное название устройства, версия устройства в семействе, кодовое название операционной системы, версия релиза, версия ядра системы, архитектура процессора, количество процессов, количество потоков.

В другом частном примере реализации параметр модуля памяти включает по меньшей мере физический размер оперативной памяти устройства.

В другом частном примере реализации параметры аккумуляторной батареи включают в себя по меньшей мере одно из: емкость батареи, максимальная емкость батареи, проектная емкость батареи.

В другом частном примере реализации алгоритм хэширования представляет собой алгоритм SHA256.

Заявленное решение также осуществляется с помощью способа выявления мошеннических транзакций, осуществляемых с помощью мобильных устройств, при этом способ содержит этапы, на которых:

с помощью АСФМ:

фиксируют регистрацию платежного приложения на мобильном устройстве;

формируют статичный идентификатор мобильного устройства;

связывают полученный идентификатор с регистрационными данными пользователя платежного приложения;

фиксируют выполнение транзакции посредством платежного приложения;

получают данные о совершении мошеннической транзакции посредством упомянутого платежного приложения;

вносят в черный список по меньшей мере полученный статичный идентификатор мобильного устройства;

блокируют работу платежного приложения на мобильном устройстве, содержащем идентификатор, внесенный в черный список.

В другом частном примере реализации фиксируют реквизиты счетов, на которые была осуществлена мошенническая транзакция.

В другом частном примере реализации выполняется внесение реквизитов счетов в черный список для последующих блокировок транзакций.

Заявленное решение также осуществляется с помощью устройства формирования статичного идентификатора мобильных устройств под управлением iOS, содержащее по меньшей мере один процессор и по меньшей мере одну память, хранящую машиночитаемые инструкции, которые при их исполнении процессором выполняют вышеуказанный способ.

Заявленное решение также осуществляется с помощью системы выявления мошеннических транзакций, содержащая по меньшей мере один процессор и по меньшей мере одну память, хранящую машиночитаемые инструкции, которые при их исполнении процессором выполняют вышеуказанный способ.

Краткое описание чертежей

Фиг. 1 иллюстрирует блок-схему способа формирования статичного идентификатора.

Фиг. 2 иллюстрирует блок-схему способа отслеживания мошеннических транзакций с помощью статичного идентификатора.

Фиг. 3 иллюстрирует схему вычислительного устройства.

Осуществление изобретения

На фиг. 1 представлена блок-схема выполнения этапов способа (100) формирования статичного идентификатора. Заявленное решение выполняется при установке платежного приложения на этапе (101) в ОС мобильного устройства. Под термином "мобильное устройство" в рамках заявленного решения может пониматься смартфон, фаблет или планшет под управлением iOS.

После установки платежного приложения, например, Сбербанк Онлайн, программная логика приложения запрашивает данные для последующей регистрации пользователя. Такими данными могут являться, ФИО, паспортные данные, номер платежной карты, номер телефона, логин/пароль для входа в приложение и т.п. Дополнительно может применяться биометрическая информация. После успешной регистрации для каждого пользователя создается уникальная запись под соответствующим идентификатором, которая сохраняется на сервере в единой базе данных.

После регистрации в приложении на этапе (102) осуществляется сбор данных мобильного устройства. Сбор осуществляется посредством программной логики платежного приложения, имеющего доступ к ОС мобильного устройства. В рамках осуществления настоящего этапа осуществляется сбор следующих параметров: параметры процессора, параметры ОС, параметры модуля памяти и параметры аккумуляторной батареи.

Данные мобильного устройства собираются по основным аппаратным модулям (процессор, память, аккумулятор), а также системные данные, идентифицирующие само устройство.

Параметры процессора могут выбираться из следующих данных, представленных в табл. 1.

Таблица 1

Параметры процессора

PROCESSOR NAME	название процессора
PROCESSOR FREQ	номинальная частота процессора
PHYSICAL CORES	количество физических ядер
LOGICAL CORES	количество логических ядер
SYSTEM	процент утилизации процессора системой
USER	процент утилизации процессора пользователем
IDLE	процент утилизации процессора в простое

Пример используемых параметров ОС приведены в табл. 2.

Таблица 2

Параметры ОС

IS PROCESS TRANSLATED	признак запуска на одном из типов устройств (нативный, транслятор, эмулятор)
ISO LANGUEGE CODE	код языка на устройстве

ISO REGION CODE	код региона на устройстве
KNOWN TIMEZONE ID	код таймзоны на устройстве
DEVICE	семейство устройств
FULL NAME	полное название устройства
VERSION	версия устройства в семействе
RELEASE	версия релиза
MACHINE	архитектура процессора
UPTIME	время, которое устройство работает после последней перезагрузки
PROCESSES	количество процессов
THREADS	количество потоков
LOAD AVERAGE	средняя загрузка операционной системы
HARDWARE ID	условно уникальный идентификатор вендора

Параметры модуля памяти могут включать в себя параметры, указанные в табл. 3.

Таблица 3

Параметры модуля памяти

PHYSICAL SIZE	физический размер оперативной памяти устройства
FREE	оперативная память, которая не используется
WIRED	количество информации, которая не может быть перемещена на жесткий диски, поэтому она должна оставаться в оперативной памяти, зависит от используемых приложений
ACTIVE	количество информации, которая в настоящее время находится в памяти и недавно использовалась
INACTIVE	количество информации в памяти, которая активно не используется, но недавно использовалась

Пример используемых параметров аккумуляторной батареи приведен в табл. 4.

Таблица 4
Параметры аккумуляторной батареи

AC POWERED	признак питания устройства переменным током
CHARGED	признак заряженности батареи
CHARGING	признак заряжается ли батарея в настоящий момент
CHARGE	процент заряженности батареи
CAPACITY	емкость батареи
MAX CAPACITY	максимальная емкость батареи
DESIGN CAPACITY	проектная емкость батареи
CYCLES	количество циклов перезарядки батареи
TEMPERATURE	текущая температура батареи

По факту сбора требуемого набора вышеуказанных параметров, на этапе (103) осуществляется их последующее хэширование с помощью, например, алгоритма SHA256.

Данный список параметров позволяет добиться:

уникальности получаемых идентификаторов, даже на одинаковых устройствах одного производителя;

неизменности идентификатора на любом устройстве, даже при минорных и мажорных обновлениях iOS;

воспроизводимости (повторяемость результатов) идентификатора при различных типах сбросов мобильного устройства до заводских и последующих восстановлений устройства.

В зависимости от типа решаемых задач идентификатор, получаемый на вышеописанных параметрах, может быть статическим и\или вероятностным, это достигается за счёт использования различных алгоритмов преобразования данных. В настоящем решении используется криптографический алгоритм хеширования SHA256. Это сделано для минимизации возможных дальнейших ограничений по сбору системных параметров со стороны iOS, а также любых других изменений, которые могут возникнуть с системными параметрами мобильного устройства во время эксплуатации (например, аппаратная замена камеры или процессора в устройстве).

На этапе (103) полученные параметры, необходимые для формирования идентификатора, формируют массив бит с помощью конкатенации их битовых значений. Массив бит может иметь следующий вид:

65 110 100 114 111 105 100 58 116 101 115 116 47 88 105 97 111 109 105 58 77 73 49 48 84 32 80 114 111 47 67 80 85 58 83 111 109 101 32 67 80 85.

Полученный массив обрабатывается генератором UUID с помощью его хеширования алгоритмом SHA256.

По итогу хеширования на этапе (104) формируется статичный идентификатор, который записывается в keychain библиотеку для данного устройства, а также в закрытую область памяти МУ. Идентификатор может иметь следующий вид: 123e4567-e89b-12d3-a456-426655440000.

Сформированный статичный идентификатор связывается с регистрационными данными пользователя, введенными в платежное приложение, и на этапе (105) передаются в базу данных на сервер. Периодичность формирования и передачи идентификаторов мобильных устройств на сервер может варьироваться в зависимости от целей и задач организации (единоразово, событийно, либо по расписанию). Полученные идентификаторы аккумулируются в автоматизированных системах организации и позволяют проводить идентификацию клиентских мобильных устройств при работе с приложением.

При выявлении аномалий (изменений) в идентификаторах клиента, банк может приостановить, либо отклонить транзакцию, как подозрительную, тем самым предотвратив возможное мошенничество (хищение денежных средств, либо имущества) в отношении клиента банка.

Уникальность заявленного подхода заключается в формировании идентификатора, одновременно сочетающего в себе несколько свойств:

статичность - устойчивый к изменениям в ОС на мобильных устройствах и не требующих дополнительных разрешений для мобильного платежного приложения;

вероятностная устойчивость - в случае изменения подхода разработчиков ОС для мобильных устройств остаются доступные характеристики, необходимые для формирования идентификатора.

Сформированная на этапе (105) информация, записанная на сервере банка, передается на этапе (106) на сервер автоматизированной системы фрод-мониторинга (АСФМ). Автоматизированная система фрод-мониторинга банка анализирует и выявляет аномалии в транзакционном потоке клиентов, помещая идентификаторы мобильных устройств злоумышленников в "чёрные" списки, тем самым предотвращая дальнейшие установки и регистрации платежных приложений на устройствах злоумышленников.

На фиг. 2 представлен пример работы способа (200) отслеживания мошеннических транзакций с помощью вышеописанного метода формирования статичного идентификатора. На первом этапе (201) АСФМ фиксирует получение сведений об осуществлении первой транзакции с помощью мобильного устройства с установленным платежным приложением, для которого уже имеется запись на сервере банка о регистрационных данных клиента и соответствующего статичного идентификатора мобильного устройства.

По факту совершенной транзакции, ее первичный статус неизвестен, и она, как правило, обрабатывается банком. Однако, при поступлении информации о том, что транзакция носила мошеннический характер (этап 202), то соответствующая запись делается в АСФМ, и для сформированного статичного идентификатора мобильного устройства, с которого была выполнена данная транзакция, формируется запись о внесении его в черный список (этап 203).

Такая ситуация может произойти в случае хищения данных клиента и их использования мошенником для регистрации платёжного приложения на своем мобильном устройстве.

При факте осуществления последующего совершения транзакции (этап 205) АСФМ осуществляет проверки соответствующего статичного идентификатора на предмет его наличия в черном списке.

Рассмотрим пример генерирования статичных идентификаторов. Статичный идентификатор первого устройства получен по следующим параметрам:

PROCESSOR NAME : A11

PROCESSOR FREQ : 2.39 GHz

PHYSICAL CORES : 6

LOGICAL CORES : 6

SYSTEM : 23

USER : 42

IDLE : 35

IS PROCESS TRANSLATED : native

ISO LANGUEGE CODE : 597

ISO REGION CODE : 256

KNOWN TIMEZONE ID : 441

DEVICE : iPhone

FULL NAME : iPhone 8 Plus

VERSION : 10.2

RELEASE : 3.95

MACHINE : ARM

UPTIME : 56078

PROCESSES : 15

THREADS : 21

LOAD AVERAGE : 34

HARDWARE ID : 9E621041-7F2E-43C3-B1A7-BCD8B5632F18

PHYSICAL SIZE : 17179869184

FREE : 1979920384

WIRED : 4351307776

ACTIVE : 4953337856

INACTIVE : 4873920512

AC POWERED : true

CHARGED : false

CHARGING : true

CHARGE : 0.83

CAPACITY : 7893

MAX CAPACITY : 7893

DESIGN CAPACITY : 1420

CYCLES : 524

TEMPERATURE : 32

SHA256 имеет вид:

D4413EB8DC76D9208F4466F42660E37DA1F737E3CA7786FEF413B492A21CAF78

UUID имеет вид:

41ffe8a2-f474-3418-80f1-1a1113336479

Статичный идентификатор второго устройства получен по следующим параметрам:

PROCESSOR NAME : A14

PROCESSOR FREQ : 3.1 GHz

PHYSICAL CORES : 6

LOGICAL CORES : 6

SYSTEM : 18

USER : 54

IDLE : 28

IS PROCESS TRANSLATED : native

ISO LANGUEGE CODE : 597

ISO REGION CODE : 256

KNOWN TIMEZONE ID : 441

DEVICE : iPhone

FULL NAME : iPhone 12 Pro Max

VERSION : 13.4

RELEASE : 3.95

MACHINE : ARM

UPTIME : 51231

PROCESSES : 12

THREADS : 15

LOAD AVERAGE : 30

HARDWARE ID : 70CD060B-B30A-46DD-A210-2771C8B80E57

PHYSICAL SIZE : 17179869184

FREE : 1979920384

WIRED : 4351307776

ACTIVE : 4953337856

INACTIVE : 4873920512

AC POWERED : true

CHARGED : false

CHARGING : true

CHARGE : 0.83

CAPACITY : 7893

MAX CAPACITY : 7893

DESIGN CAPACITY : 1420

CYCLES : 524

TEMPERATURE : 32

SHA256 имеет вид:

8899FE3A92BE1EF6446E415E025B9B7C40E2F76F0351A7C34044D810C5CED8A1

UUID имеет вид:

48ec3487-d1bc-3444-abb1-c4c03e49bc31

Полученные статичные идентификаторы записываются в защищенную память каждого из мобильных устройств.

При этом, если фиксируется появление нового идентификатора у одного и того же пользователя, но при этом статичный UUID идентификатор говорит о том, что новый идентификатор очень похож на предыдущий, то это позволяет дополнительно учитывать такие изменения в системе фрод-мониторинга и более быстро реагировать на возможные попытки мошеннической активности.

На этапе (206) по факту выполненной проверки АСФМ принимается решение о блокировке или одобрению транзакции. В случае ее блокировки и расценивании действий как мошеннических на сервере банка выполняется определение также транзакционных реквизитов мошенников, на основании информации о совершенной транзакции, что позволяет как эффективно блокировать последующие установки платежных приложений (при сравнении статичного идентификатора с ранее внесенным в черный список), так и мошеннических реквизитов для предотвращения поступления на них средств.

На фиг. 3 представлен общий вид вычислительной системы, реализованной на базе вычислительного устройства (300). В общем случае, вычислительное устройство (300) содержит объединенные общей шиной информационного обмена один или несколько процессоров (301), средства памяти, такие как ОЗУ (302) и ПЗУ (303), интерфейсы ввода/вывода (304), устройства ввода/вывода (305), и устройство для сетевого взаимодействия (306).

Процессор (301) (или несколько процессоров, многоядерный процессор) могут выбираться из ассортимента устройств, широко применяемых в текущее время, например, компаний Intel™, AMD™, Apple™, Samsung Exynos™, MediaTEK™, Qualcomm Snapdragon™ и т.п. Под процессором также необходимо учитывать графический процессор, например, GPU NVIDIA или ATI, который также является пригодным для полного или частичного выполнения способа (100). При этом, средством памяти может выступать доступный объем памяти графической карты или графического процессора. ОЗУ (302) представляет собой оперативную память и предназначено для хранения исполняемых процессором (301) машиночитаемых инструкций для выполнение необходимых операций по логической обработке данных. ОЗУ (302), как правило, содержит исполняемые инструкции операционной системы и соответствующих программных компонент (приложения, программные модули и т.п.).

ПЗУ (303) представляет собой одно или более устройств постоянного хранения данных, например, жесткий диск (HDD), твердотельный накопитель данных (SSD), флэш-память (EEPROM, NAND и т.п.), оптические носители информации (CD-R/RW, DVD-R/RW, BlueRay Disc, MD) и др.

Для организации работы компонентов устройства (300) и организации работы внешних подключаемых устройств применяются различные виды интерфейсов В/В (304). Выбор соответствующих интерфейсов зависит от конкретного исполнения вычислительного устройства, которые могут представлять собой, не ограничиваясь: PCI, AGP, PS/2, IrDa, FireWire, LPT, COM, SATA, IDE, Lightning, USB (2.0, 3.0, 3.1, micro, mini, type C), TRS/Audio jack (2.5, 3.5, 6.35), HDMI, DVI, VGA, Display Port, RJ45, RS232 и т.п. Для обеспечения взаимодействия пользователя с вычислительным устройством (300) применяются различные средства (305) В/В информации, например, клавиатура, дисплей (монитор), сенсорный дисплей, тач-пад, джойстик, манипулятор мышь, световое перо, стилус, сенсорная панель, трекбол, динамики, микрофон, средства дополненной реальности, оптические сенсоры, планшет, световые индикаторы, проектор, камера, средства биометрической идентификации (сканер сетчатки глаза, сканер отпечатков пальцев, модуль распознавания голоса) и т.п.

Средство сетевого взаимодействия (306) обеспечивает передачу данных устройством (300) посредством внутренней или внешней вычислительной сети, например, Интранет, Интернет, ЛВС и т.п. В качестве одного или более средств (306) может использоваться, но не ограничиваться: Ethernet карта, GSM модем, GPRS модем, LTE модем, 5G модем, модуль спутниковой связи, NFC модуль, Bluetooth и/или BLE модуль, Wi-Fi модуль и др.

Дополнительно могут применяться также средства спутниковой навигации в составе устройства (300), например, GPS, ГЛОНАСС, BeiDou, Galileo.

Представленные материалы заявки раскрывают предпочтительные примеры реализации технического решения и не должны трактоваться как ограничивающие иные, частные примеры его воплощения, не выходящие за пределы испрашиваемой правовой охраны, которые являются очевидными для специалистов соответствующей области техники.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ формирования статичного идентификатора мобильных устройств под управлением iOS, содержащий этапы, на которых с помощью процессора мобильного устройства:

устанавливают платежное приложение в операционную систему (ОС) мобильного устройства;

осуществляют запуск платежного приложения и регистрацию пользователя в нем, при этом осуществляют сбор параметров мобильного устройства, включающих в себя: параметры процессора, параметры ОС, параметры модуля памяти и параметры аккумуляторной батареи;

осуществляют конкатенирование полученных параметров;

формируют массив бит на основе конкатенации параметров;

выполняют хэширование полученного массива бит;

формируют статичный идентификатор мобильного устройства на основании выполненного хэширования;

записывают полученный статичный идентификатор в закрытую область памяти мобильного устройства;

связывают полученный идентификатор с платежным приложением конкретного пользователя;

передают полученный идентификатор на сервер автоматизированной системы фрод-мониторинга (АСФМ).

2. Способ по п.1, характеризующийся тем, что параметры процессора включают по меньшей мере одно из: название процессора, номинальная частота процессора, количество физических ядер, количество логических ядер, процент утилизации процессора системой, процент утилизации процессора пользователем, процент утилизации процессора в простое.

3. Способ по п.1, характеризующийся тем, что параметры ОС включают по меньшей мере одно из: признак запуска, код языка на устройстве, код региона на устройстве, код таймзоны на устройстве, семейство устройств, полное название устройства, версия устройства в семействе, кодовое название операционной системы, версия релиза, версия ядра системы, архитектура процессора, количество процессов, количество потоков.

4. Способ по п.1, характеризующийся тем, что параметр модуля памяти включает по меньшей мере физический размер оперативной памяти устройства.

5. Способ по п.1, характеризующийся тем, что параметры аккумуляторной батареи включают в себя по меньшей мере одно из: емкость батареи, максимальная емкость батареи, проектная емкость батареи.

6. Способ по п.1, характеризующийся тем, что алгоритм хэширования представляет собой алгоритм SHA256.

7. Способ выявления мошеннических транзакций, осуществляемых с помощью мобильных устройств, при этом способ содержит этапы, на которых с помощью АСФМ:

фиксируют регистрацию платежного приложения на мобильном устройстве;

формируют статичный идентификатор мобильного устройства по любому из пп.1-6;

связывают полученный идентификатор с регистрационными данными пользователя платежного приложения;

фиксируют выполнение транзакции посредством платежного приложения;

получают данные о совершении мошеннической транзакции посредством упомянутого платежного приложения;

вносят в черный список по меньшей мере полученный статичный идентификатор мобильного устройства;

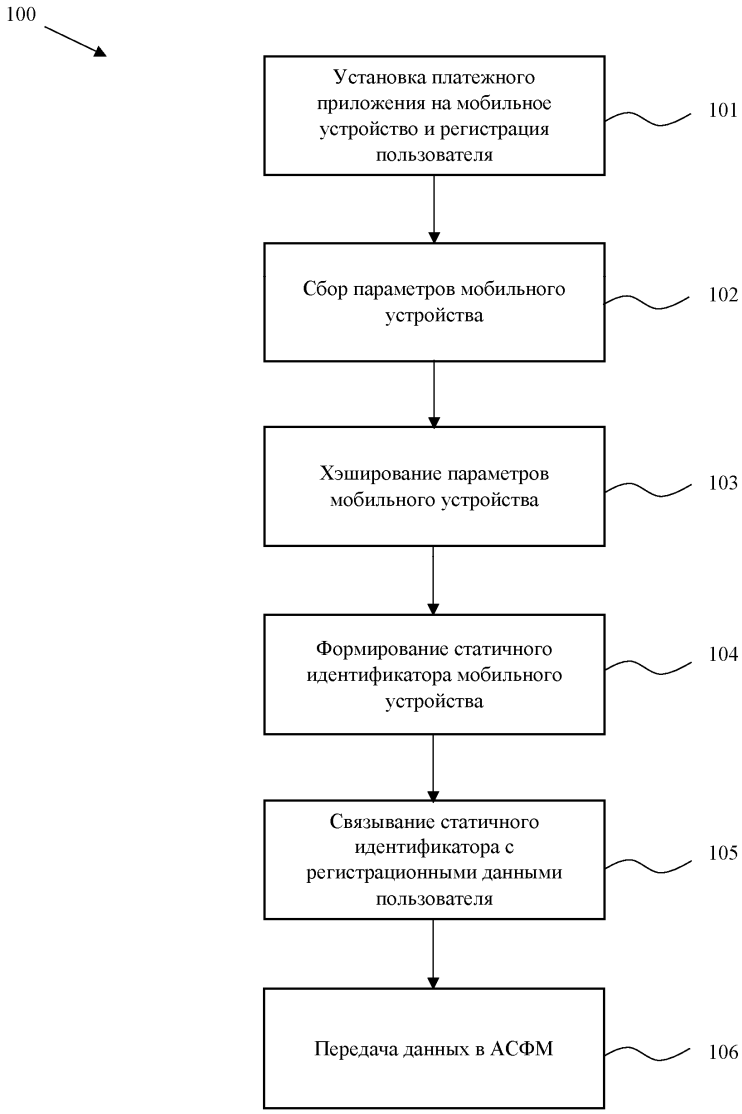
блокируют работу платежного приложения на мобильном устройстве, содержащем идентификатор, внесенный в черный список.

8. Способ по п.7, характеризующийся тем, что фиксируют реквизиты счетов, на которые была осуществлена мошенническая транзакция.

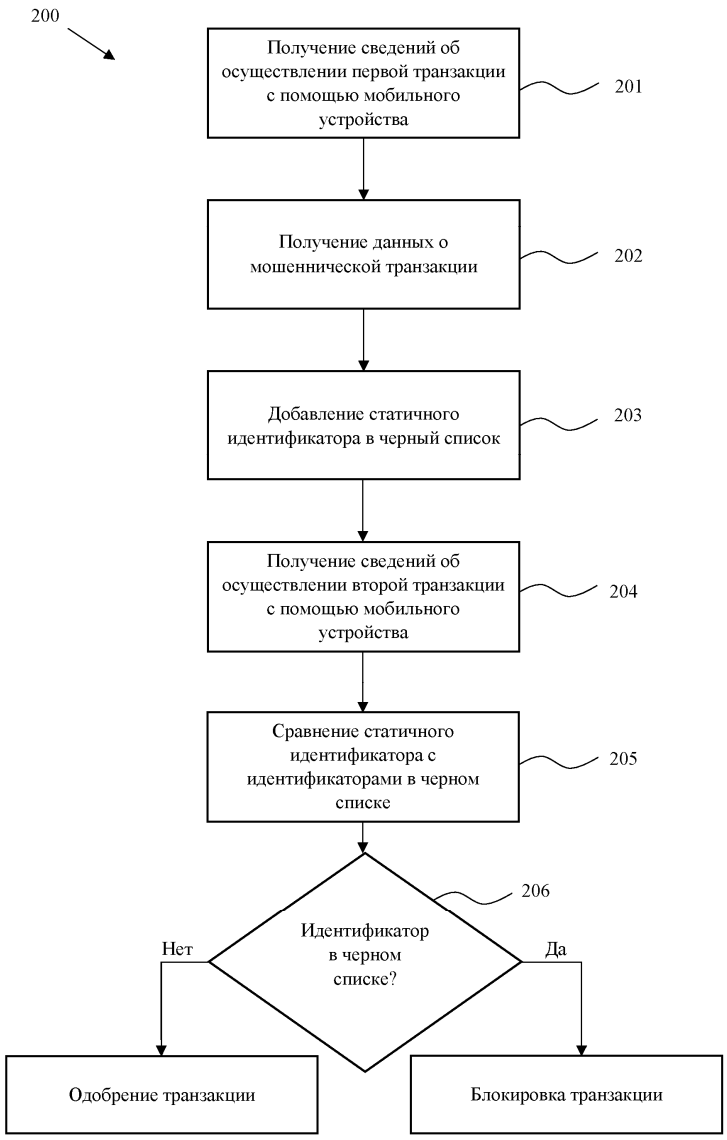
9. Способ по п.8, характеризующийся тем, что выполняется внесение реквизитов счетов в черный список для последующих блокировок транзакций.

10. Устройство формирования статичного идентификатора мобильных устройств под управлением iOS, содержащее по меньшей мере один процессор и по меньшей мере одну память, хранящую машиночитаемые инструкции, которые при их исполнении процессором выполняют способ по любому из пп.1-6.

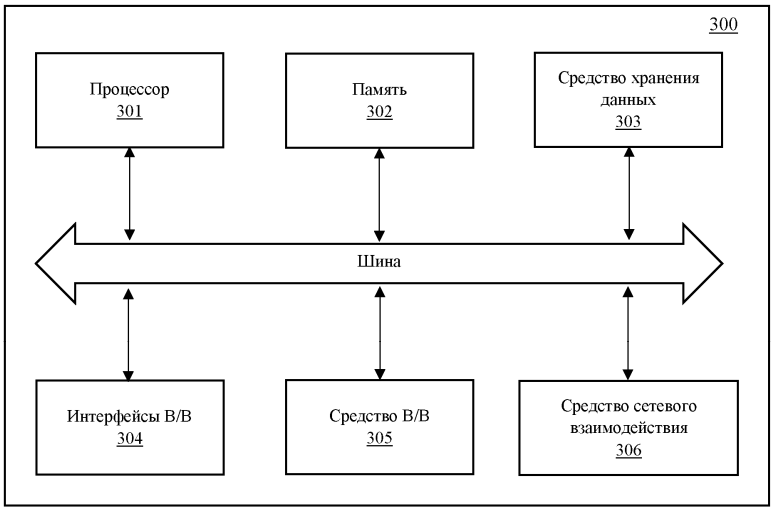
11. Система выявления мошеннических транзакций, содержащая по меньшей мере один процессор и по меньшей мере одну память, хранящую машиночитаемые инструкции, которые при их исполнении процессором выполняют способ по любому из пп.7-9.


100
Установка платежного приложения на мобильное устройство и регистрация пользователя
101
Сбор параметров мобильного устройства
102
Хэширование параметров мобильного устройства
103
Формирование статичного идентификатора мобильного устройства
104
Связывание статичного идентификатора с регистрационными данными пользователя
105
Передача данных в АСФМ
106

Фиг. 1



Фиг. 2



Фиг. 3

Евразийская патентная организация, ЕАПВ
Россия, 109012, Москва, Малый Черкасский пер., 2