РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 649 793**(13) **C2**

(51) МПК
G06F 21/31 (2013.01)
G06F 15/18 (2006.01)
G06F 21/00 (2013.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
G06F 21/00 (2006.01); G06F 21/30 (2006.01); G06F 21/316 (2006.01)

(21)(22) Заявка: **2016131909, 03.08.2016**

(24) Дата начала отсчета срока действия патента:
03.08.2016

Дата регистрации:
04.04.2018

Приоритет(ы):
(22) Дата подачи заявки: **03.08.2016**

(43) Дата публикации заявки: **08.02.2018** Бюл. № 4

(45) Опубликовано: **04.04.2018** Бюл. № 10

Адрес для переписки:
143026, Москва, Территория инновационного центра Сколково, ул. Нобеля, 5, оф. 402.1, ООО "ЦИС "Сколково"

(72) Автор(ы):
Крылов Павел Владимирович (RU),
Сачков Илья Константинович (RU)

(73) Патентообладатель(и):
ООО "Группа АйБи" (RU)

(56) Список документов, цитированных в отчете о поиске: **US 8677472 B1, 18.03.2014. US 2011/0023115 A1, 27.01.2011. US 2006/0224898 A1, 05.10.2006. RU 2530210 C2, 27.06.2014.**

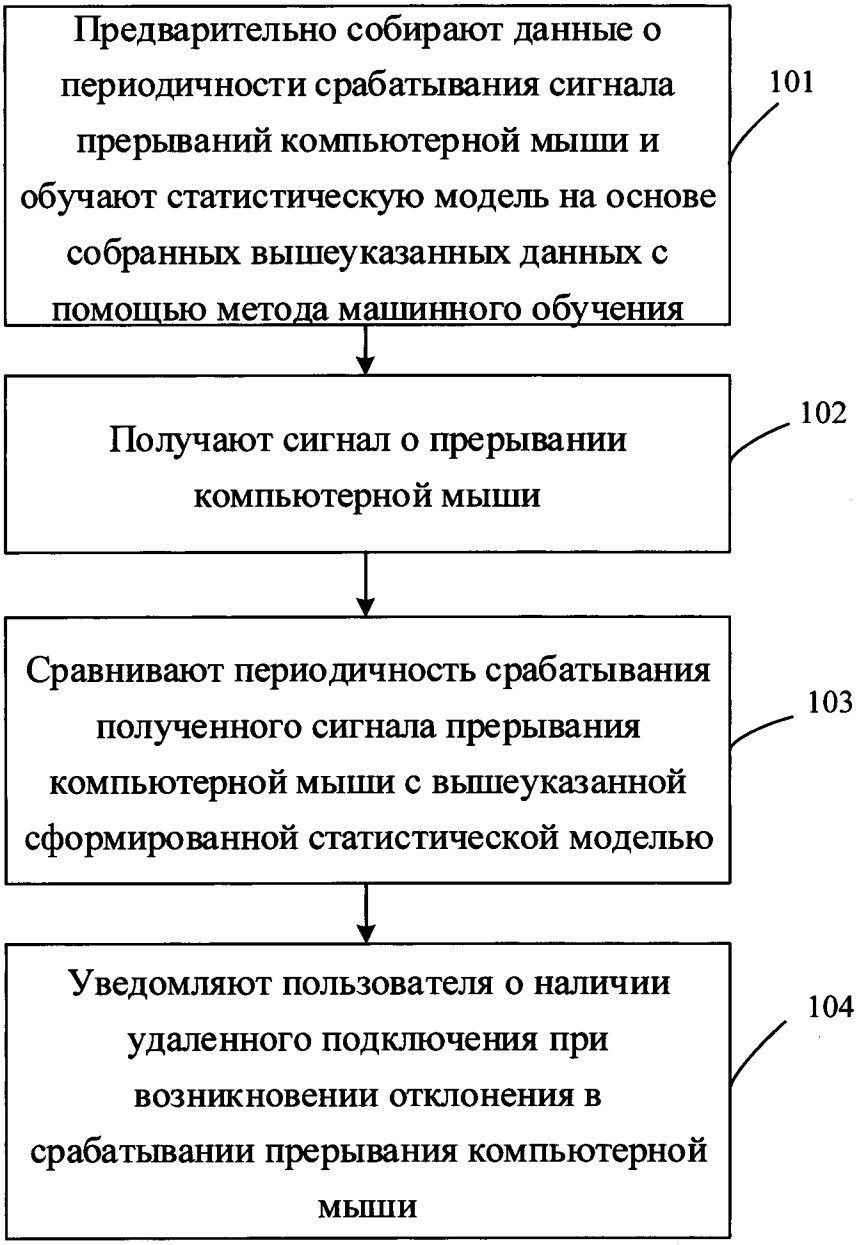
(54) СПОСОБ И СИСТЕМА ВЫЯВЛЕНИЯ УДАЛЕННОГО ПОДКЛЮЧЕНИЯ ПРИ РАБОТЕ НА СТРАНИЦАХ ВЕБ-РЕСУРСА

(57) Реферат:

Изобретение относится к области вычислительной техники. Технический результат заключается в расширении арсенала средств выявления удаленного подключения на основе данных о срабатывании и прерывании компьютерной мыши. Способ при работе на страницах веб-ресурса включает этапы, на которых предварительно собирают данные о периодичности срабатывания события движения компьютерной мыши, получают события движения компьютерной мыши, сравнивают периодичность срабатывания полученного события движения компьютерной мыши с вышеуказанной сформированной статистической моделью, при возникновении отклонения в срабатывании события движения компьютерной мыши уведомляют владельца защищаемого веб-ресурса о наличии удаленного подключения у посетителя веб-ресурса для последующего реагирования на стороне владельца. 2 н. и 2 з.п. ф-лы, 4 ил.

RU 2649793 C2

RU 2649793 C2



Фиг. 1

RU 2649793 C2

RU 2649793 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 649 793**(13) **C2**

(51) Int. Cl.
G06F 21/31 (2013.01)
G06F 15/18 (2006.01)
G06F 21/00 (2013.01)

(12) ABSTRACT OF INVENTION

(52) CPC
G06F 21/00 (2006.01); G06F 21/30 (2006.01); G06F 21/316 (2006.01)

(21)(22) Application: **2016131909, 03.08.2016**

(24) Effective date for property rights:
03.08.2016

Registration date:
04.04.2018

Priority:
(22) Date of filing: **03.08.2016**

(43) Application published: **08.02.2018** Bull. № **4**

(45) Date of publication: **04.04.2018** Bull. № **10**

Mail address:
143026, Moskva, Territoriya innovatsionnogo tsentra Skolkovo, ul. Nobelya, 5, of. 402.1, OOO "TSIS "Skolkovo"

(72) Inventor(s):
Krylov Pavel Vladimirovich (RU),
Sachkov Ilya Konstantinovich (RU)

(73) Proprietor(s):
OOO "Gruppa AjBi" (RU)

(54) METHOD AND SYSTEM OF DETECTING REMOTE CONNECTION WHEN WORKING ON WEB RESOURCE PAGES

(57) Abstract:

FIELD: computer engineering.

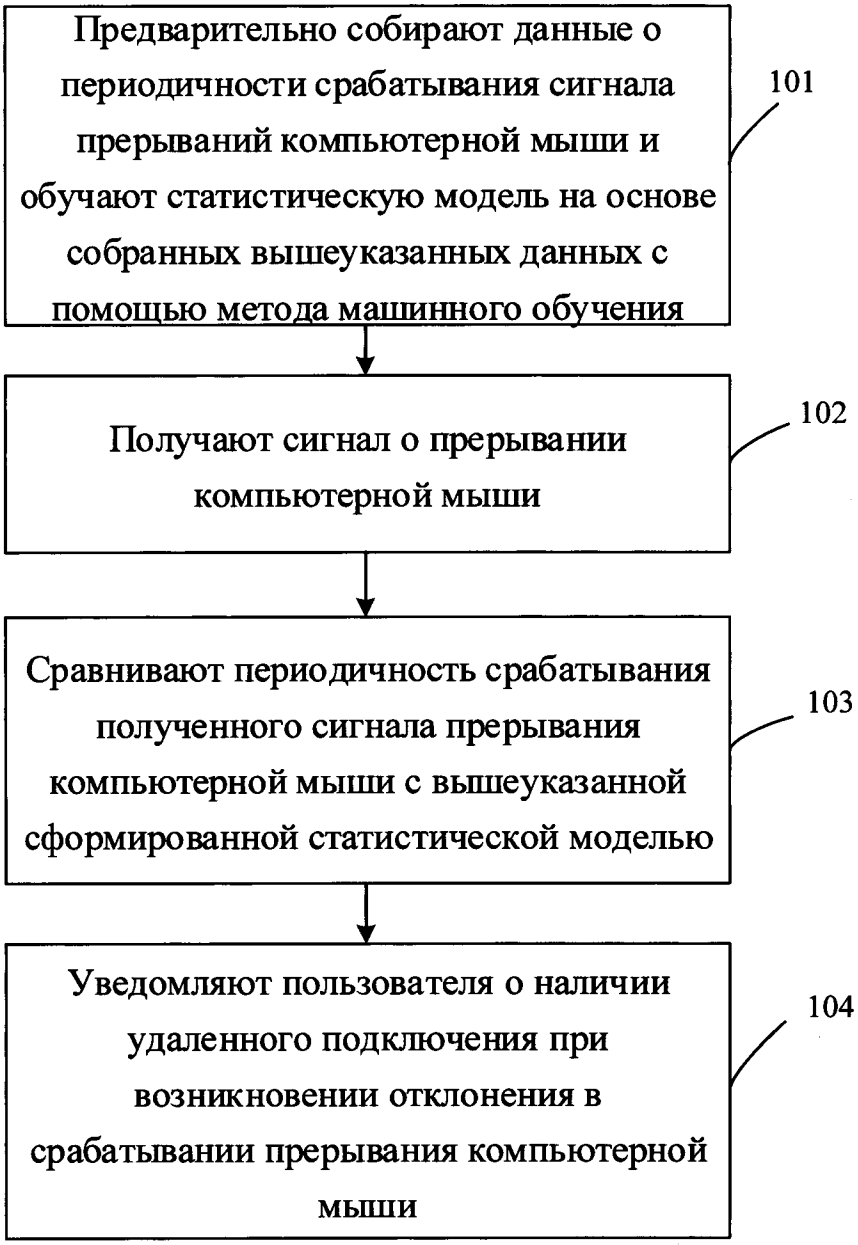
SUBSTANCE: invention relates to computer engineering. Method when working on the pages of a web resource includes the steps of pre-gathering data on the timing of a computer mouse event, gather the computer mouse events, compare the frequency of operation of the received computer mouse event with the above-mentioned generated statistical model, if there is a deviation in the operation of the computer mouse event, the owner of the protected web resource is notified that there is a remote connection from the visitor of the web resource for the subsequent response to the owner's side.

EFFECT: technical result consists in expanding the arsenal of means of detecting a remote connection based on data on the operation and interruption of a computer mouse.

4 cl, 4 dwg

RU 2649793 C2

RU 2649793 C2



Фиг. 1

RU 2649793 C2

RU 2649793 C2

ОБЛАСТЬ ТЕХНИКИ

[0001] Данное техническое решение относится к области вычислительной техники, а точнее к способам и системам выявления удаленного доступа при работе на страницах веб-ресурса.

УРОВЕНЬ ТЕХНИКИ

[0002] С недавних времен использование электронных ключей (токенов) и смарт-карт, с неизвлекаемыми криптографическими ключами, с помощью которых производится подписание юридически значимых документов и денежных переводов, перестало считаться надежным способом защиты от мошенников. Самой распространенной схемой обхода этих средств является использование вредоносного программного обеспечения для несанкционированного сбора учетных данных, пин-кодов, паролей на устройстве «жертвы» с последующим удаленным доступом на его устройство и совершение действий в информационных системах от имени легитимного пользователя.

[0003] Подобные атаки перестали быть единичными, и особенно широкое применение получили у кибермошенников при хищении денежных средств через различные системы онлайн-платежей и дистанционного банковского обслуживания. Для осуществления удаленного доступа часто используются такие общедоступные программы как Microsoft Remote Desktop, TeamViewer, Lite Manager, Ammyy Admin, Remote Admin, семейство на основе VNC.

[0004] Самым известным способом выявления использования средств удаленного доступа является фиксирование изменения параметров экрана, таких как его ширина и высота, а также глубина цветности. Например, при удаленном управлении с использованием Microsoft Remote Desktop, по умолчанию используются параметры экрана, с которого осуществляется удаленный доступ. Эти экранные параметры доступны через JavaScript, и соответственно могут быть считаны при доступе пользователя на веб-ресурс. Данным способом пользуется широкий спектр антифрод-решений, таких как ThreatMetrix, RSA Transaction Monitoring, NICE Actimize, Kaspersky Fraud Prevention и другие.

[0005] Однако в случае использования Microsoft Remote Desktop мошенник может явно установить необходимые параметры экрана, а при использовании других средств удаленного доступа, таких как VNC, Ammyy Admin, TeamViewer, эти параметры по умолчанию будут соответствовать параметрам экрана управляемого устройства. В этом случае удаленное подключение вышеописанным способом не будет выявлено, в чем заключается его существенный недостаток.

СУЩНОСТЬ

[0006] Данное изобретение направлено на устранение недостатков, присущих существующим решениям.

[0007] Технической проблемой в данном техническом решении является выявление удаленного подключения при работе на страницах веб-ресурса без использования специальных программ, а только с использованием средств браузера.

[0008] Техническим результатом является расширение арсенала технических средств для выявления удаленного подключения на основе данных о срабатывании прерывания компьютерной мыши.

[0009] Указанный технический результат достигается благодаря способу выявления удаленного подключения при работе на страницах веб-ресурса, в котором предварительно собирают данные о периодичности срабатывания сигнала прерываний компьютерной мыши и обучают статистическую модель на основе собранных

вышеуказанных данных с помощью метода машинного обучения; получают сигнал о прерывании компьютерной мыши; сравнивают периодичность срабатывания полученного сигнала прерывания компьютерной мыши с вышеуказанной сформированной статистической моделью; выявляют наличие удаленного подключения при возникновении отклонения в срабатывании прерывания компьютерной мыши.

[00010] Также указанный технический результат достигается благодаря системе выявления удаленного подключения при работе на страницах веб-ресурса, содержащая: сервер, выполненный с возможностью сбора данных о периодичности срабатывания сигнала прерываний компьютерной мыши, а также обучения статистической модели на основе полученных вышеуказанных данных с помощью метода машинного обучения и сравнения периодичности срабатывания полученного сигнала прерывания компьютерной мыши с вышеуказанной сформированной статистической моделью; сервер удаленного доступа, выполненный с возможностью получения сигнала от компьютерной мыши от клиента удаленного доступа; клиент удаленного доступа, выполненный с возможностью передачи сигнала о прерывании компьютерной мыши на сервер удаленного доступа; компьютерную мышку; браузер, выполненный с возможностью загрузки скрипта для сбора и передачи данных о периодичности срабатывания сигнала прерывания компьютерной мыши на устройстве пользователя.

[00011] В некоторых вариантах осуществления технического решения данными о периодичности срабатывания события движения компьютерной мыши являются медиана и дисперсия распределения набора временных замеров (в мс) между соседними вызовами события движения мыши.

[00012] В некоторых вариантах осуществления технического решения при обучении статической модели на основе выбранных данных используют такой метод машинного обучения, как метод k-ближайших соседей или линейную регрессию.

[00013] В некоторых вариантах осуществления технического решения при обучении статической модели на основе выбранных данных используют аппроксимирующие функции для вычисления параметров, необходимых для выявления использования средства удаленного доступа.

[00014] Технический результат достигает следующим способом. Известные в уровне техники способы выявления удаленного подключения без использования агентского решения, которые могут анализировать открываемые порты и протоколы общения, состоят в выявлении факта смены разрешения экрана или глубины цвета. Например, при штатной работе пользователя за устройством А экран имеет разрешение 1024 на 768 пикселей, и глубину цвета 32 бита. При удаленном подключении с использованием RDP (Remote Desktop Protocol) по умолчанию клиент удаленного управления использует разрешение экрана устройства Б, с которого происходит доступ, а не устройства А. В результате изменяется разрешение экрана и, например, с использованием JavaScript из браузера это можно определить. Значение глубины цвета также может быть снижено относительно оригинального значения в целях снижения объема трафика между управляющим и управляемым устройствами.

[00015] К сожалению, данные способы не срабатывают в большинстве реальных случаев. Во-первых, не сработает против осторожных мошенников, которые имеют возможность получить оригинальное значение разрешения и глубины цвета, и выставить их вручную в параметрах клиента удаленного доступа. Во-вторых, такие широко используемые системы удаленного доступа как VNC, TeamViewer, LiteManager, Remote Admin, Ammyy Admin не изменяют по умолчанию ни разрешения, ни глубины цвета.

[00016] Данное техническое решение предлагает новый способ выявления удаленного

подключения, который определяет использование всех вышеперечисленных программ удаленного подключения за счет учета фундаментальных принципов их работы.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[00017] Признаки и преимущества настоящего изобретения станут очевидными из приводимого ниже подробного описания изобретения и прилагаемых чертежей, на которых:

[00018] На Фиг. 1 показан примерный вариант осуществления технического решения согласно способу выявления удаленного подключения при работе на страницах веб-ресурса;

[00019] На Фиг. 2 показан примерный вариант осуществления технического решения согласно системе выявления удаленного подключения при работе на страницах веб-ресурса;

[00020] На Фиг. 3 показан примерный вариант осуществления технического решения согласно способу выявления удаленного подключения при работе на страницах веб-ресурса. На диаграмме показаны существенные компоненты, участвующие при работе легитимного пользователя со своего устройства на страницах веб-ресурса. Также показана последовательность взаимодействия компонент для первичного построения статистической модели и последующей проверки данных прерывания компьютерной мыши.

[00021] На Фиг. 4 показан примерный вариант осуществления технического решения согласно способу выявления удаленного подключения при работе на страницах веб-ресурса. На диаграмме показаны существенные компоненты, участвующие при использовании средств удаленного доступа и вносящие аномальные изменения в данные прерывания компьютерной мыши. Также показана последовательность взаимодействия компонент для выявления использования средств удаленного управления (обозначены сокращением УУ).

ПОДРОБНОЕ ОПИСАНИЕ

[00022] Данное техническое решение может быть реализовано на компьютере, в виде системы или машиночитаемого носителя, содержащего инструкции для выполнения вышеупомянутого способа.

[00023] Техническое решение может быть реализовано в виде распределенной компьютерной системы.

[00024] В данном решении под системой подразумевается компьютерная система, ЭВМ (электронно-вычислительная машина), ЧПУ (числовое программное управление), ПЛК (программируемый логический контроллер), компьютеризированные системы управления и любые другие устройства, способные выполнять заданную, четко определенную последовательность операций (действий, инструкций).

[00025] Под устройством обработки команд подразумевается электронный блок либо интегральная схема (микропроцессор), исполняющая машинные инструкции (программы).

[00026] Устройство обработки команд считывает и выполняет машинные инструкции (программы) с одного или более устройства хранения данных. В роли устройства хранения данных могут выступать, но, не ограничиваясь, жесткие диски (HDD), флеш-память, ПЗУ (постоянное запоминающее устройство), твердотельные накопители (SSD), оптические приводы.

[00027] Программа - последовательность инструкций, предназначенных для исполнения устройством управления вычислительной машины или устройством обработки команд.

[00028] Ниже будут описаны термины и понятия, необходимые для осуществления настоящего технического решения.

[00029] Статистическая модель - модель, описывающая (в большей или меньшей степени) взаимосвязь между признаками (переменными).

[00030] Машинное обучение - обширный подраздел искусственного интеллекта, математическая дисциплина, использующая разделы математической статистики, численных методов оптимизаций, теории вероятностей, дискретного анализа и извлекающая знания из данных.

[00031] Прерывание - сигнал, сообщающий процессору о наступлении какого-либо события. При этом выполнение текущей последовательности команд приостанавливается и управление передается обработчику прерывания, который реагирует на событие и обслуживает его, после чего возвращает управление в прерванный код.

[00032] Сервер - компьютер и/или оборудование для выполнения на нем сервисного программного обеспечения (в том числе серверов тех или иных задач).

[00033] Сервер удаленного доступа обеспечивает пользователя через соответствующую клиентскую программу аналогом локального терминала (текстового или графического) для работы на удаленной системе. Для обеспечения доступа к командной строке служат серверы telnet, RSH и SSH. Для обеспечения доступа к графическому терминалу (оболочке) используются такие программы, как RDP, VNC, TeamViewer, RemoteAdmin, AmmyyAdmin, LiteManager.

[00034] Браузер - прикладное программное обеспечение для просмотра веб-страниц; содержания веб-документов, компьютерных файлов и их каталогов; управления веб-приложениями; а также для решения других задач.

[00035] Компьютерная мышь - механический манипулятор, преобразующий движение в управляющий сигнал. В частности, сигнал может быть использован для позиционирования курсора или прокрутки страниц.

[00036] ДБО - дистанционное банковское обслуживание.

[00037] В информатике и программировании событие - это сообщение программного обеспечения (либо его части), которое указывает, что произошло.

[00038] Согласно заявляемому техническому решению способ выявления удаленного подключения при работе на страницах веб-ресурса, который показан на Фиг. 1, реализован следующим образом.

[00039] Шаг 101: предварительно собирают данные о периодичности срабатывания сигнала прерываний компьютерной мыши и обучают статистическую модель на основе собранных вышеуказанных данных с помощью метода машинного обучения.

[00040] Данными являются медиана и дисперсия распределения набора временных замеров (в мс) между соседними вызовами события движения мышки. Набор замеров имеет фиксированную длину. Данный шаг выполняется при первых сеансах работы пользователя в браузере при посещении защищаемого веб-ресурса. Вместе с веб-ресурсом в браузер клиента загружается JavaScript-код, который производит сбор периодичности прерывания компьютерной мышки и передает их обратно на веб-сервер для накопления и последующего анализа. Аналогичный подход может быть реализован в любом приложении или его расширении, которое не имеет возможности контролировать открытые порты на устройстве пользователя. Например, если приложение реализовано как flash (ActionScript) и запускается в браузере, можно использовать ровно тот же способ. Подразумевается, что мошенник еще не атаковал пользователя, и полученная в ходе обучения статистическая модель будет отражать работу пользователя локально за своим вычислительным устройством. Для построения

статистической модели используются методы машинного обучения на основе данных о периодичности срабатывания компьютерной мышки.

[00041] В качестве методов машинного обучения могут быть использованы метод k-ближайших соседей, линейная регрессия, и иные алгоритмы кластеризации и выявления аномалий. В условиях ограниченного набора данных о событии движения мыши возможно использование аппроксимирующих функций для вычисления необходимых параметров для выявления использования средства удаленного доступа. Под ограниченным набором данных понимается, что как правило, сессия работы мошенника под удаленным управлением довольно короткая (1-2 минуты). Его задача, например, быстро создать платеж и уйти. В этих условиях можно не набрать достаточное количество данных. Поэтому используется аппроксимация на основе тех данных, которые успели накопиться. Например, в качестве такой функции может выступать дисперсия распределения из N случайных величин, которые необходимы для достоверного определения использования удаленного подключения, может быть аппроксимирована функцией a/(N^2)+b, где коэффициенты a и b - вычисляются на основе дисперсий от меньшего количества случайных величин, полученных в ходе сессии работы на защищаемом веб-ресурсе.

[00042] Шаг 102: получают события движения компьютерной мыши;

[00043] Шаг 103: сравнивают периодичность срабатывания полученного сигнала прерывания компьютерной мыши с вышеуказанной сформированной статистической моделью.

[00044] В общем случае сравнивается набор полученных данных, т.к. и при нормальной работе могут быть одиночные выбросы (аномалии)

[00045] Выявляет разницу периодичности прерывания компьютерной мыши со статистической моделью, построенной на этапе обучения. Если она оказывается статистически значимой, то принимается решение, что наличествует удаленное подключение. На основе полученных данных о периодичности прерывания компьютерной мыши и статистической модели, построенной алгоритмом выявления аномалий на этапе обучения, принимается решение, что наличествует удаленное управление.

[00046] Шаг 104: при возникновении отклонения в срабатывании прерывания компьютерной мыши уведомляют владельца защищаемого веб-ресурса о наличии удаленного подключения у посетителя веб-ресурса для последующего реагирования на стороне владельца. В качестве реагирования может быть, например, ограничение доступа к функционалу веб-ресурса, дополнительной авторизации клиента, прерывании сессии работы с посетителем или отзыве ранее совершенных действий, и т.п.

[00047] Важно, что уведомляется не пользователь, а владелец веб-ресурса (банк в случае ДБО). Бессмысленно показывать что-либо в браузере под удаленным управлением мошенника.

[00048] Рассмотрим пример осуществления технического решения.

[00049] JavaScript-код регистрирует свой обработчик на событие window.onmousemove браузера. Обработчик вызывается браузером при передвижении мышки.

[00050] В обработчике при каждом вызове замеряется разница между временем предыдущего вызова и текущего. Используется промежуточный массив счетчиков с индексами от 0 до заданного количества (например, 40). При каждом вызове обработчика увеличивается на единицу счетчик с индексом равным разнице времени предыдущего вызова и текущего. По достижении заданного количества последовательно полученных разниц времен, подсчитывается медиана. Эти значения медианы

отправляются на сервер. Массив счетчиков обнуляется, и вся описанная выше итерация повторяется.

[00051] На сервере полученные значения медианы накапливаются до заданного количества - на этом этапе накапливаются данные, которые относятся к классу «пользователь работает локально». Заданное количество задается настройками алгоритма выявления аномалий и представляет собой положительное число, например 100, как показано в примере реализации ниже. По получении заданного количества медиан вычисляется следующая статистическая модель.

[00052] Среднее значение медианы m и ее дисперсия sd.

[00053] Задается пороговое значение большее m+3*sd*K, где K - является настроечным параметром, задающим чувствительность выявления. В пределах [0, m+3*sd) находится 0.07% всего нормального распределения медиан, данный интервал взят из теории статистики.

[00054] Например, в ходе нескольких сессий локальной работы клиента в ДБО были получены следующие значения медианы (в миллисекундах):

[00055] [9, 10, 11, 11, 11, 9, 11, 10, 11, 11, 11, 11, 11, 11, 11, 9, 9, 11, 11, 9, 11, 11, 11, 11, 12, 13, 13, 12, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 11, 11, 11, 11, 11, 10, 9, 11, 11, 11, 11, 11, 11, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 13, 13, 13, 13, 13, 13, 11, 11, 11, 11, 11, 11, 9, 9, 9, 9, 9, 9, 9]

[00056] m=10.09

[00057] sd=1.295641

[00058] при K=1, пороговое значение равно 13.97692

[00059] После этого все получаемые значения медианы тестируются на вхождение в промежуток [0, m+3*sd*K]. Если медиана выходит за пределы, то считается, что происходит удаленное управление. Это имеет очень простой физический смысл: при плавном движении мышки на стороне мошенника сигналы от нее передаются от клиента удаленного доступа на сервер удаленного доступа с некоторой большей периодичностью (задержкой), что на управляемом устройстве выглядит как дерганое движение мышки (большими скачками).

[00060] Поскольку события window.onmousemove обрабатываются в общей очереди событий однопоточной (single threaded) JavaScript-машины браузера, то аномалии возможны и при локальной работе. Поэтому при оценке одиночные выбросы не учитываются. При удаленной работе аномальные значения медианы идут группами.

[00061] Например, в ходе сессии работы через TeamViewer были получены следующие значения медиан: [41, 41, 41, 41, 41]

[00062] 41 - значит, что реальные медианы вышли за пределы массива счетчиков, т.е. задержки были более 40 мс.

[00063] В результате среднее из этих медиан выходит за пределы допустимого значения 13.97692.

[00064] Этим способом выявляются такие средства удаленного доступа как RDP и TeamViewer. Другие средства удаленного доступа требуют других алгоритмов выявления основанных на изменении дисперсии периодичности срабатывания событий window.onmousemove.

[00065] Согласно заявляемому техническому решению система выявления удаленного подключения при работе на страницах веб-ресурса, реализована следующим образом.

[00066] Сервер выполнен с возможностью сбора данных о периодичности срабатывания сигнала прерываний компьютерной мыши, а также обучения статистической модели на основе полученных вышеуказанных данных с помощью

метода машинного обучения и сравнения периодичности срабатывания полученного сигнала прерывания компьютерной мыши с вышеуказанной сформированной статистической моделью.

[00067] Все подробности реализации сбора данных о периодичности срабатывания сигнала прерываний компьютерной мыши, а также обучение статистической модели на основе полученных данных описаны выше.

[00068] В любом домене узлы потребителей, серверы, магистральные соединения и т.п. рассматриваются как «локальные» для этого домена, в то время как эти элементы в пределах другого домена рассматриваются как «удаленные».

[00069] сервер удаленного доступа, выполненный с возможностью получения сигнала от компьютерной мыши от клиента удаленного доступа;

[00070] клиент удаленного доступа, выполненный с возможностью передачи сигнала о прерывании компьютерной мыши на сервер удаленного доступа;

[00071] компьютерная мышка;

[00072] браузер, выполненный с возможностью загрузки скрипта для сбора и передачи данных о периодичности срабатывания сигнала прерывания компьютерной мыши на устройстве пользователя.

[00073] Специалист в данной области техники может легко осуществить другие варианты изобретения из рассмотренного описания, раскрытого здесь. Эта заявка предназначена для того, чтобы покрыть любые варианты изобретения, и включая такие отклонения от настоящего изобретения, которые появляются в пределах известной или обычной практики в уровне техники. Предполагается, что описание и примеры рассматриваются только как примерные, с сущностью и объемом настоящего изобретения, обозначенные формулой технического решения.

[00074] Следует принимать во внимание, что настоящее раскрытие не ограничивается точными конструкциями, которые были описаны выше и проиллюстрированы на прилагаемых чертежах, и что различные модификации и изменения могут быть сделаны без отхода от области его применения. Предполагается, что объем технического решения ограничен только прилагаемой формулой.

(57) Формула изобретения

1. Способ выявления удаленного подключения при работе на страницах веб-ресурса, содержащий:

- предварительно собирают данные о периодичности срабатывания события движения компьютерной мыши, при этом данными о периодичности срабатывания события движения компьютерной мыши являются медиана и дисперсия распределения набора временных замеров между соседними вызовами события движения мыши, и обучают статистическую модель на основе собранных вышеуказанных данных с помощью метода машинного обучения;
- получают события движения компьютерной мыши;
- сравнивают периодичность срабатывания полученного события движения компьютерной мыши с вышеуказанной сформированной статистической моделью;
- при возникновении отклонения в срабатывании события движения компьютерной мыши, уведомляют владельца защищаемого веб-ресурса о наличии удаленного подключения у посетителя веб-ресурса для последующего реагирования на стороне владельца.

2. Способ по п. 1, характеризующийся тем, что при обучении статической модели на основе выбранных данных используют такой метод машинного обучения, как метод

k-ближайших соседей или линейную регрессию.

3. Способ по п. 1, характеризующийся тем, что при обучении статической модели на основе выбранных данных используют аппроксимирующие функции для вычисления параметров, необходимых для выявления использования средства удаленного доступа.

4. Система выявления удаленного подключения при работе на страницах веб-ресурса, содержащая:

- сервер, выполненный с возможностью сбора данных о периодичности срабатывания сигнала прерываний компьютерной мыши, а также обучения статистической модели на основе полученных вышеуказанных данных с помощью метода машинного обучения и сравнения периодичности срабатывания полученного сигнала прерывания компьютерной мыши с вышеуказанной сформированной статистической моделью, при этом данными о периодичности срабатывания события движения компьютерной мыши являются медиана и дисперсия распределения набора временных замеров между соседними вызовами события движения мыши;

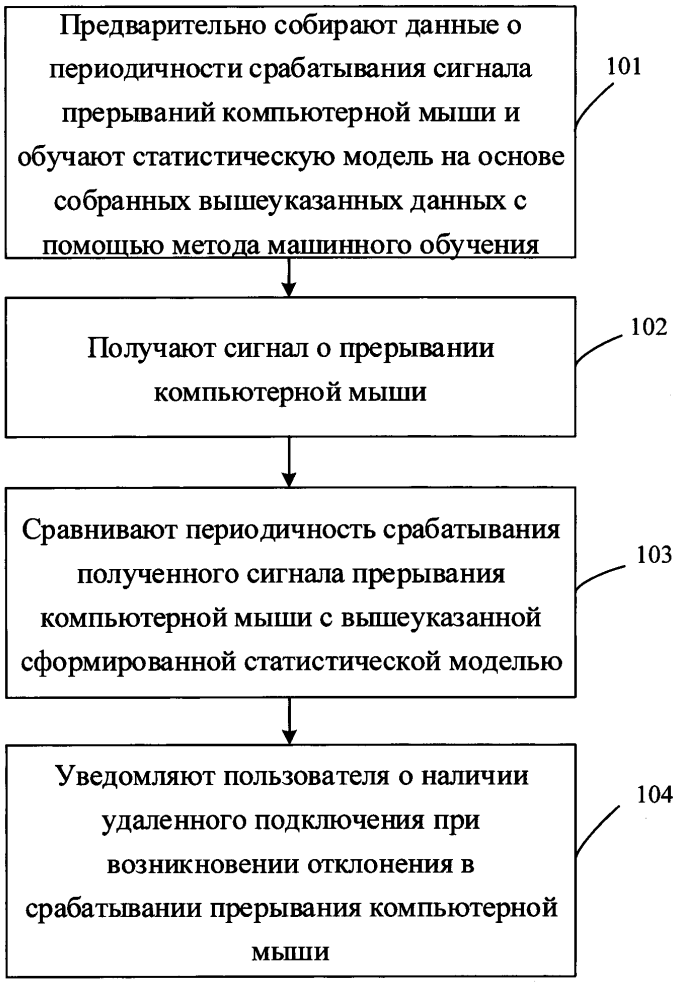
- сервер удаленного доступа, выполненный с возможностью получения сигнала от компьютерной мыши от клиента удаленного доступа;

- клиент удаленного доступа, выполненный с возможностью передачи сигнала о прерывании компьютерной мыши на сервер удаленного доступа;

- компьютерная мышка;

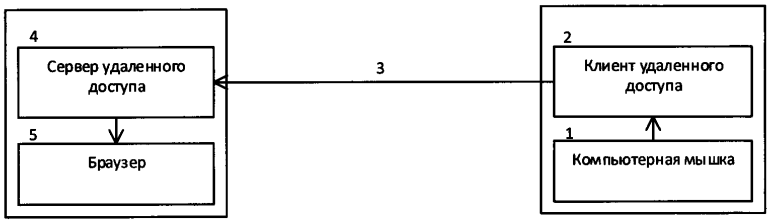
- браузер, выполненный с возможностью загрузки скрипта для сбора и передачи данных о периодичности срабатывания сигнала прерывания компьютерной мыши на устройстве пользователя.

1


Предварительно собирают данные о периодичности срабатывания сигнала прерываний компьютерной мыши и обучают статистическую модель на основе собранных вышеуказанных данных с помощью метода машинного обучения
101
Получают сигнал о прерывании компьютерной мыши
102
Сравнивают периодичность срабатывания полученного сигнала прерывания компьютерной мыши с вышеуказанной сформированной статистической моделью
103
Уведомляют пользователя о наличии удаленного подключения при возникновении отклонения в срабатывании прерывания компьютерной мыши
104

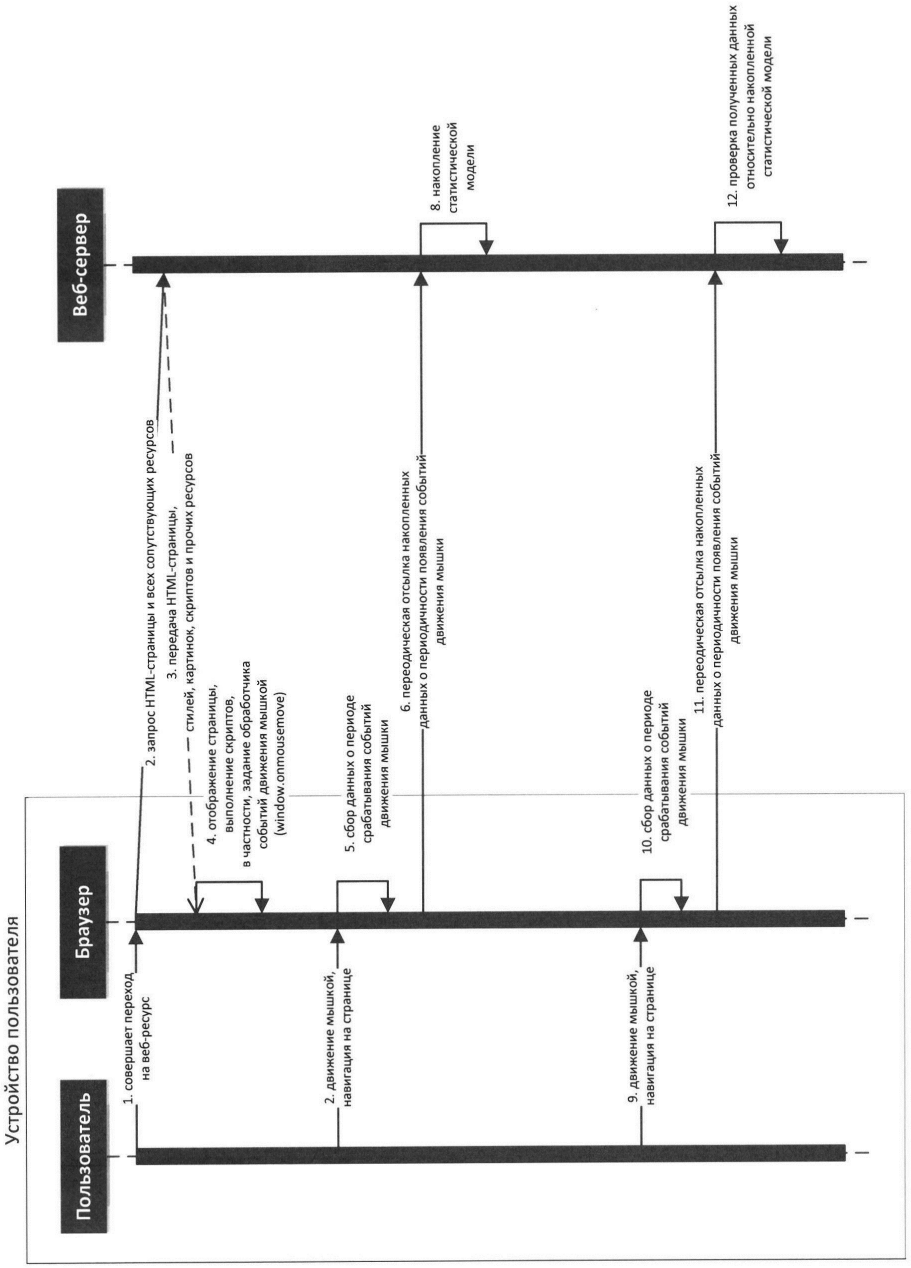
Фиг. 1

2


4
Сервер удаленного доступа
5
Браузер
3
2
Клиент удаленного доступа
1
Компьютерная мышка

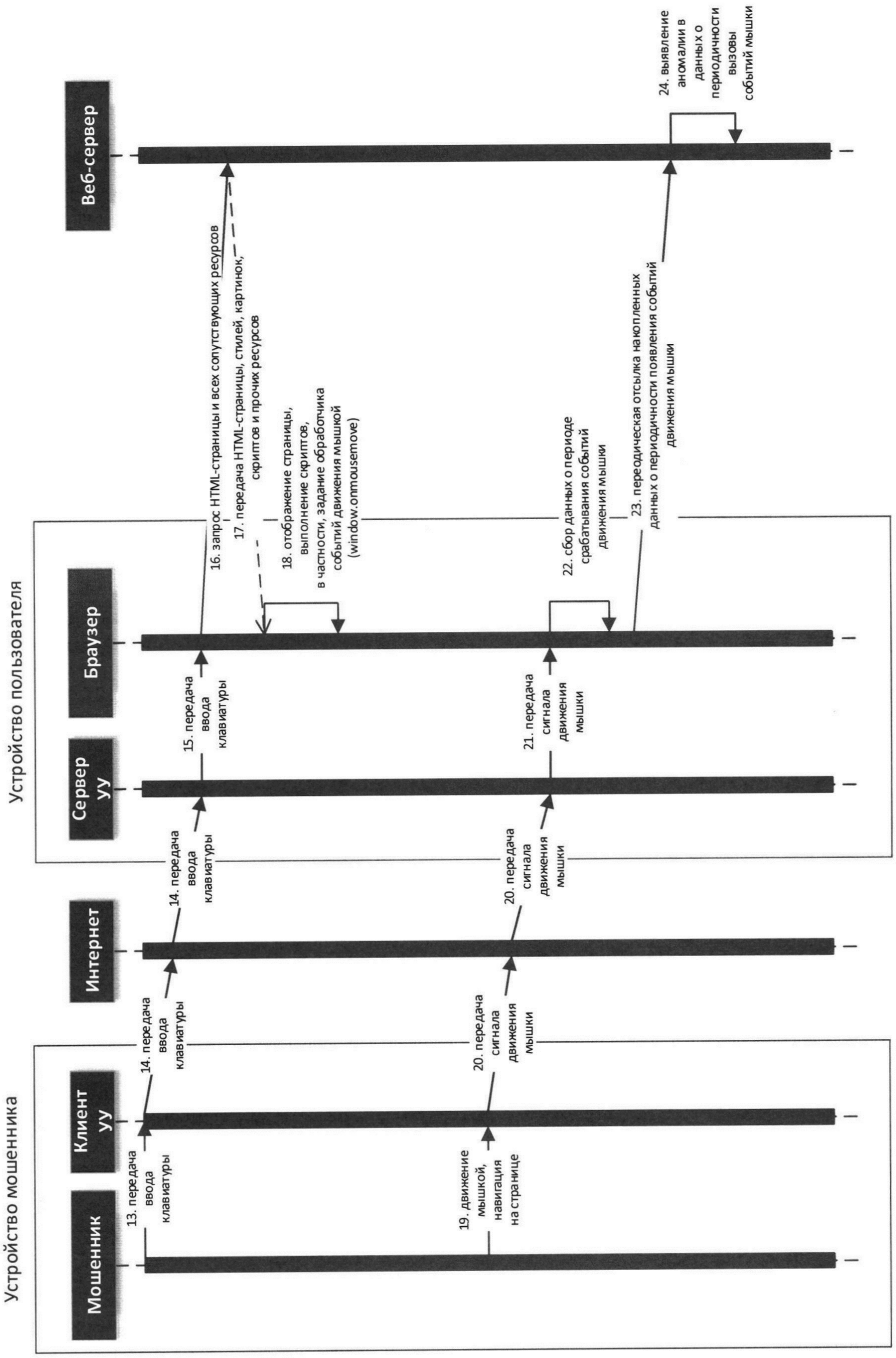
Фиг. 2

3


Устройство пользователя
Пользователь
Браузер
Веб-сервер
1. совершает переход на веб-ресурс
2. запрос HTML-страницы и всех сопутствующих ресурсов
3. передача HTML-страницы, стилей, картинок, скриптов и прочих ресурсов
4. отображение страницы, выполнение скриптов, в частности, задание обработчика событий движения мышкой (window.onmousemove)
2. движение мышкой, навигация на странице
5. сбор данных о периоде срабатывания событий движения мышки
6. переодическая отсылка накопленных данных о периодичности появления событий движения мышки
8. накопление статистической модели
9. движение мышкой, навигация на странице
10. сбор данных о периоде срабатывания событий движения мышки
11. переодическая отсылка накопленных данных о периодичности появления событий движения мышки
12. проверка полученных данных относительно накопленной статистической модели

Фиг. 3

4


Устройство мошенника
Устройство пользователя
Мошенник
Клиент уу
Интернет
Сервер уу
Браузер
Веб-сервер
13. передача ввода клавиатуры
14. передача ввода клавиатуры
14. передача ввода клавиатуры
15. передача ввода клавиатуры
16. запрос HTML-страницы и всех сопутствующих ресурсов
17. передача HTML-страницы, стилей, картинок, скриптов и прочих ресурсов
18. отображение страницы, выполнение скриптов, в частности, задание обработчика событий движения мышкой (window.onmousemove)
19. движение мышкой, навигация на странице
20. передача сигнала движения мышки
20. передача сигнала движения мышки
21. передача сигнала движения мышки
22. сбор данных о периоде срабатывания событий движения мышки
23. переодическая отсылка накопленных данных о периодичности появления событий движения мышки
24. выявление аномалии в данных о периодичности вызовы событий мышки

Фиг. 4