

(12) МЕЖДУНАРОДНАЯ ЗАЯВКА, ОПУБЛИКОВАННАЯ В
СООТВЕТСТВИИ С ДОГОВОРом О ПАТЕНТНОЙ КООПЕРАЦИИ (РСТ)

(19) Всемирная Организация
Интеллектуальной Собственности
Международное бюро

(43) Дата международной публикации
08 февраля 2018 (08.02.2018)



(10) Номер международной публикации
WO 2018/026303 A1

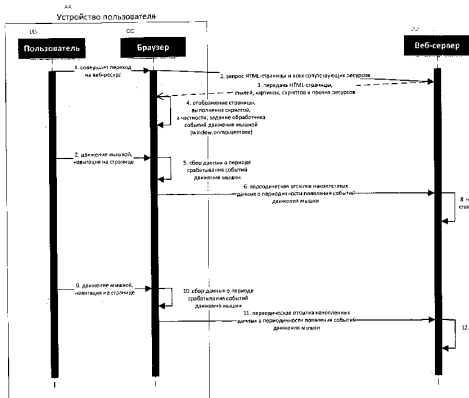
- (51) Международная патентная классификация:
G06F 21/31 (2013.01) **G06F 15/18** (2006.01)
- (21) Номер международной заявки: PCT/RU2016/000526
- (22) Дата международной подачи:
09 августа 2016 (09.08.2016)
- (25) Язык подачи: Русский
- (26) Язык публикации: Русский
- (30) Данные о приоритете:
2016131909 03 августа 2016 (03.08.2016) RU
- (71) Заявитель: **ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ГРУППА АЙ-БИ" (OBSHESTVO S OGRANICHENNOI OTVETSTVENNOSTYU "GROUP-IB")** [RU/RU]; ул.

Шарикоподшипниковская, 1, эт. 9, к. 2 Москва, 115088, Moscow (RU).

- (72) Изобретатели: **КРЫЛОВ, Павел Владимирович (KRYLOV, Pavel Vladimirovich)**; Коровинское шоссе, 23, корп. 1, кв. 113 Москва, 125412, Moscow (RU). **САЧКОВ, Илья Константинович (SACHKOV, Ilya Konstantinovich)**; Измайловский б-р, 34, кв. 136 Москва, 105043, Moscow (RU).
- (74) Агент: **КОТЛОВ, Дмитрий Владимирович (KOTLOV, Dmitry Vladimirovich)**; ООО "ЦИС "Сколково", Территория инновационного центра "Сколково", 4, офис 402.1, Москва, 143026, Moscow (RU).
- (81) Указанные государства (если не указано иначе, для каждого вида национальной охраны): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,

(54) Title: METHOD AND SYSTEM FOR DETECTING REMOTE ACCESS DURING ACTIVITY ON THE PAGES OF A WEB RESOURCE

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



Фиг. 3

AA User device
BB User
CC Browser
DD Web server
1 Transition made to web resource
2 HTML page and all accompanying resources requested
3 HTML page, styles, images, scripts and other resources transmitted
4 Page displayed, scripts executed, in particular mousemove event processor act
5 Mousemove, navigation on page
6 Data about rate of mousemove events collected
7 Stored data about rate of mousemove events periodically sent
8 Statistical model stored
9 Mousemove, navigation on page
10 Data collected about the rate of occurrence of a mousemove signal
11 Stored data about rate of mousemove events periodically sent
12 Received data checked against statistical model

(57) Abstract: The present invention relates to the field of computer technology, and more particularly to methods and systems for detecting remote access during activity on the pages of a web resource. A method for detecting remote access during activity on the pages of a web resource includes the following steps: initially collecting data about the rate of occurrence of a mouse interrupt signal, and training a statistical model on the basis of data collected, using a machine learning method; receiving a mouse interrupt signal; comparing the rate of occurrence of the received mouse interrupt signal with the aforesaid statistical model; and notifying the user of the presence of remote access in the event of an aberration in the occurrence of the mouse interrupt signal. The technical result is more accurate remote access detection on the basis of data about the occurrence of a mouse interrupt signal.

(57) Реферат: Данное техническое решение относится к области вычислительной техники, а точнее к способам и системам выявления удаленного доступа при работе на страницах веб-ресурса. Способ выявления удаленного подключения при работе на страницах веб-ресурса, содержит следующие шаги: 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; уведомляют пользователя о наличии удаленного подключения при возникновении отклонения в срабатывании прерывания компьютерной мыши. Технический результат - повышение точности выявления подключения удаленного доступа на основе данных о срабатывании прерывания компьютерной мыши.

[продолжение на следующей странице]

WO 2018/026303 A1

CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Указанные государства (если не указано иначе, для каждого вида региональной охраны): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), евразийский (AM, AZ, BY, KG, KZ, RU, TJ, TM), европейский патент (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Опубликована:

— с отчётом о международном поиске (статья 21.3)