

METHOD AND SYSTEM OF REMOTE CONNECTION DETECTION WHEN WORKING ON WEB RESOURCE PAGES

5 FIELD

[0001] This technical solution refers to the field of computer science, and particularly to the methods and systems of remote access detection when working on web resource pages.

BACKGROUND

10 **[0002]** Recently, the use of electronic keys (tokens) and smart cards with non-recoverable cryptographic keys, which are used to sign legally significant documents and money transfers, has ceased to be considered a reliable method of protection against fraudsters. The most common scheme to bypass these means is the use of malicious software for unauthorized collection of login information, PIN codes,
15 passwords on the “victim’s” device, followed by remote access to his/her device and performing actions in information systems on behalf of the legitimate user.

[0003] Such attacks have ceased to be isolated and are particularly widely used by cyber fraudsters in the theft of money through various online payment systems and remote banking services. Such publicly available programs as Microsoft Remote
20 Desktop, TeamViewer, Lite Manager, Ammyy Admin, Remote Admin, a VNC-based family are often used for remote access.

[0004] The most known method to detect the use of remote access means is to record changes in screen parameters, such as its width and height, as well as colour depth. For example, in case of remote control using Microsoft Remote Desktop, the
25 default screen settings from which remote access is performed are used. These screen parameters are accessible through JavaScript, and can be read when the user accesses the web resource accordingly. This method uses a wide range of antifraud

solutions, such as ThreatMetrix, RSA Transaction Monitoring, NICE Actimize, Kaspersky Fraud Prevention, etc.

[0005] However, in case of Microsoft Remote Desktop use, the fraudster can explicitly set the necessary screen parameters, and when using other remote access tools such as VNC, Ammyy Admin, TeamViewer, these default parameters will correspond to the screen settings of the controlled device. In this case, the remote connection using the said method will not be revealed, and this is its significant disadvantage.

SUMMARY

[0006] This technology is aimed at elimination of disadvantages inherent to the existing solutions.

[0007] The technical problem in this technical solution is the identification of a remote connection when working on the web resource pages without special programs, and using browser tools only.

[0008] The technical result is the expansion of the technical means range for remote connection detection based on data concerning the computer mouse interrupt.

[0009] The said technical result is achieved due to the method of remote connection detection when working on the web resource pages, wherein data on the periodicity of the computer mouse interrupt signal are preliminarily collected and a statistical model is trained on the basis of the said data collected using the machine learning method; a signal concerning computer mouse interrupt is received; the periodicity of the received computer mouse interrupt signal is compared with the said-formed statistical model; the presence of a remote connection is determined in the event of a deviation in the computer mouse interrupt.

[00010] This technical result is also achieved due to the system of remote connection detection when working on the web resource pages, the system comprising: a server configured to collect data on the periodicity of the computer mouse interrupt signal, as well as statistical model training based on the said data using the machine learning method and comparison of the periodicity of the received

computer mouse interrupt signal with the said statistical model; remote access server, configured to receive a signal from a computer mouse from a remote access client; remote access client, configured for the possibility of transmitting a signal concerning the computer mouse interrupt to a remote access server; computer mouse; a browser configured to load a script for collecting and transmitting data on the periodicity of computer mouse interrupt signal on a user's device.

[00011] In some embodiments of the technical solution, the data on the periodicity of computer mouse movement event are the median and the dispersion of the time measurements set distribution (in ms) between adjacent calls of a mouse movement event.

[00012] In some embodiments of the technical solution, when training a static model based on selected data, the machine learning method such as the k-nearby neighbours method or linear regression is used.

[00013] In some embodiments of the technical solution, when training a static model based on selected data, the approximating functions for calculating the parameters necessary for detecting the use of remote access means are used.

[00014] The technical result is achieved as follows. Current methods of remote connection detection known in the prior art without the use of an agent solution that can analyse the ports being opened and the communication protocols consist in identifying whether the screen resolution or colour depth has changed. For example, in case of normal use of device A by the user, the screen has a resolution of 1024 x 768 pixels and a colour depth of 32 bits. In case of remote connection using RDP (Remote Desktop Protocol), by default, the remote control client uses the screen resolution of device B from which the access is performed, not device A. As a result, the screen resolution changes and, for example, this can be determined using JavaScript from a browser. The value of the colour depth can also be reduced in respect to the original value in order to reduce the amount of traffic between the control and the controlled devices.

[00015] Unfortunately, these methods do not work in most of real cases. Firstly, it will not work against cautious fraudsters who have the ability to receive the

original resolution and colour depth values and manually set them in the parameters of the remote access client. Secondly, such widely used remote access systems as VNC, TeamViewer, LiteManager, Remote Admin, Ammyy Admin do not change neither resolution nor colour depth by default.

- 5 **[00016]** This technical solution offers a new way to identify a remote connection, which defines the use of all the said remote connection programs by taking into account the fundamental principles of their work.

BRIEF DESCRIPTON OF THE DRAWINGS

- 10 **[00017]** Features and advantages of this technology will become obvious from the below detailed description and accompanying drawings, namely, wherein:

[00018] Fig. 1 shows an exemplary embodiment of the technical solution according to the method of remote connection detection when working on the web resource pages;

- 15 **[00019]** Fig. 2 shows an exemplary embodiment of the technical solution according to the system of remote connection detection when working on the web resource pages;

[00020] Fig. 3 shows an exemplary embodiment of the technical solution according to the method of remote connection detection when working on the web resource pages. The diagram shows the essential components involved in the operation of a legitimate user from his/her device on the web resource pages. It also shows the sequence of components interaction for the primary construction of a statistical model and the subsequent verification of the data of a computer mouse interrupt.

- 25 **[00021]** Fig. 4 shows an exemplary embodiment of the technical solution according to the method of remote connection detection when working on the web resource pages. The diagram shows the essential components involved in using remote access means and making anomalous changes to the computer mouse

interrupt data. It also shows the sequence of interaction of components to identify the use of remote control means (indicated by the RC abbreviation).

DETAILED DESCRIPTION

[00022] This technical solution can be implemented on a computer, in the form of a system or a machine-readable medium containing instructions for using the said method.

[00023] The technical solution can be implemented as a distributed computer system.

[00024] In this technical solution, the system means a computer system, PC (personal computer), CNC (computer numeric control), PLC (programmable logic controller), computerized control system and any other devices that can perform defined, clearly determined sequences of operations (actions, instructions).

[00025] Command processing device - an electronic unit or integral circuit (microprocessor) which executes machine instructions (programs).

[00026] A command processing device reads and executes machine instructions (programs) received from one or more data storage devices. Data storage devices include but are not limited to hard drives (HDD), flash memory, ROM (read-only memory), solid-state drives (SSD), optic drives.

[00027] Program means a sequence of instructions intended for execution by computer control device or command processing devices.

[00028] The terms and concepts required to implement this technical solution will be described below.

[00029] **Statistical model** - a model that describes (to a greater or lesser extent) the relationship between features (variables).

[00030] **Machine learning** — an extensive subdivision of artificial intelligence, a mathematical discipline using sections of mathematical statistics, numerical optimization methods, probability theory, discrete analysis, and extracting knowledge from data.

[00031] **Interrupt** — a signal informing the processor of the occurrence of an event. Wherein the execution of the current command sequence is suspended and control is transferred to the interrupt handler, which responds to the event, handle it, and then returns control to the interrupted code.

5 [00032] **Server** — computer and/or equipment for service software execution (including servers of various tasks).

[00033] **Remote access server** provides the user with an analogue of a local terminal (text or graphic) to work on the remote system through the appropriate client program. Telnet, RSH and SSH servers are used to provide access to the
10 command line. To provide access to the graphic terminal (shell), such programs as RDP, VNC, TeamViewer, RemoteAdmin, AmmyyAdmin, LiteManager are used.

[00034] **Browser** — application software for web pages, web documents content, computer files and their folders viewing; web application management; as well as for other tasks.

15 [00035] **Computer mouse** — a mechanical manipulator that transforms movement into a control signal. In particular, the signal can be used to position the cursor or scroll through pages.

[00036] **RBS** – remote banking service.

[00037] In computer science and programming, an **event** is a message from a
20 software (or part of it) that indicates what happened.

[00038] According to the claimed technical solution, the method of remote connection detection when working on the web resource pages, which is shown in Figure 1, is implemented as follows:

[00039] **Step 101:** the data on the periodicity of the computer mouse interrupt
25 signal are preliminarily collected and a statistical model is trained on the basis of the said data collected using the machine learning method.

[00040] The data are represented by the median and the dispersion of the time measurements set distribution (in ms) between adjacent calls of a mouse movement event. The set of measurements has a fixed length. This step is performed during the
30 first user sessions in the browser when visiting a protected web resource. Along with

the web resource, JavaScript code is loaded into the client browser, which collects the periodicity of computer mouse interrupts and sends them back to the web server for accumulation and subsequent analysis. A similar approach can be implemented in any application or its extension, which does not have the ability to control open ports on the user's device. For example, if an application is implemented as flash (ActionScript) and runs in a browser, you can use exactly the same method. It is understood that the fraudster has not yet attacked the user, and the statistical model obtained during the training will reflect the user's work locally on his computing device. To build a statistical model, machine learning methods are used based on the periodicity of the computer mouse response.

[00041] The k-nearby neighbours method or linear regression are used as methods of machine learning, as well as other clustering and anomaly detection algorithms. In conditions of limited data concerning the mouse movement event, it is possible to use approximating functions to calculate the necessary parameters for detecting the use of remote access means. A limited data set means that, as a rule, a fraudster's session under a remote control is rather short (1–2 minutes). His task is, for example, to quickly create a payment and leave. Under these conditions, you cannot collect enough data. Therefore, approximation is used based on the data that have been accumulated. For example, such a function may be represented by the distribution dispersion of N random variables that are necessary to reliably determine the use of remote connection, which can be approximated by the function $a/(N^2) + b$, where the a and b coefficients are calculated on the basis of variances from a smaller number of random variables obtained during a session of work on a protected web resource.

[00042] **Step 102:** computer mouse movement events are received;

[00043] **Step 103:** the periodicity of the received computer mouse interrupt signal is compared with the said formed statistical model.

[00044] In general, the data set is compared, because there may be single emissions (anomalies) during normal operation.

[00045] The difference between the periodicity of computer mouse interrupt and a statistical model built at the training step is identified. If it turns out to be statistically significant, then a decision is made that there is a remote connection. On the basis of the data obtained on the periodicity of computer mouse interrupt and the statistical model built by the anomaly detection algorithm at the training step, a decision is made that there is a remote control.

[00046] **Step 104:** in case of deviation in computer mouse interrupt the owner of the protected web resource is notified of the presence of a remote connection of the visitor of the web resource for subsequent response from the owner's side. As a response, there may be, for example, restriction of access to the functionality of a web resource, additional authorization of a client, interrupt of a session for a visitor or recall of previously performed actions, etc.

[00047] It is important that not the user is notified, but the owner of the web resource (the bank in the case of RBS). It makes no sense to show anything in the browser under the remote control of the fraudster.

[00048] An example of the technical solution embodiment is below.

[00049] JavaScript code registers its handler for window.onmousemove browser event. The handler is called by the browser when the mouse is moving.

[00050] At each call, the difference between the time of the previous call of the interrupt and the current one is measured in the handler. An intermediate array of counters with indices from 0 to a specified number (for example, 40) is used. Each time the handler is called, the counter with an index equal to the time difference between the previous call and the current one is incremented by one. Upon reaching a specified number of successively obtained time differences, the median is calculated. These median values are sent to the server. The array of counters is reset, and the entire iteration described above is repeated.

[00051] On the server, the resulting values of the median are accumulated up to the specified number - at this step, the data that belongs to the "user works locally" class are accumulated. The specified number is set by the anomaly detection algorithm settings and is a positive number, for example 100, as shown in the

example of embodiment below. Upon receipt of a given number of medians, the following statistical model is calculated:

[00052] The average value of the median m and its variance sd ;

[00053] A threshold value greater than $m+3*sd*K$ is set, where K – is a setting parameter defining detection sensitivity. Only 0.07% of the total normal distribution of medians is within the range of $[0, m+3*sd)$, this interval is taken from statistical theory.

[00054] For example, during several sessions of the local client operation in the RBS, the following median values were obtained (in milliseconds):

[00055] [9, 10, 11, 11, 11, 9, 11, 10, 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, 11, 11, 11, 11, 11, 10, 9, 11, 11, 11, 11, 11, 11, 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] when $K = 1$, the threshold value is 13.97692

[00059] After that, all median values obtained are tested for being within the interval of $[0, m+3*sd*K]$. If the median is out of range, then remote control is considered to take place. It has a very simple physical meaning: in case of a smooth mouse movement on the side of the fraudster, the signals from it are transmitted from the remote access client to the remote access server with some greater periodicity (delay), which looks like a jerky mouse movement (great leaps) on the controlled device.

[00060] Since `window.onmousemove` events are processed in the common event queue of a single threaded JavaScript machine of the browser, anomalies are possible even during local operation. Therefore, single emissions are not taken into account during estimation. When working remotely, the anomalous values of the median come in groups.

[00061] For example, during a work session via TeamViewer, the following median values were obtained: [41, 41, 41, 41, 41]

[00062] 41 means that the real medians are beyond the array of counters, i.e. delays were more than 40 ms.

[00063] As a result, the average of these medians is outside the range of 13.97692.

5 [00064] This method identifies such remote access means as RDP and TeamViewer. Other remote access means require other detection algorithms based on the change in the variance of the window.onmousemove event frequency.

[00065] According to the claimed technical solution, the system of remote connection detection when working on the web resource pages is implemented as
10 follows:

[00066] A server is configured to collect data on the periodicity of the computer mouse interrupt signal as well as statistical model training based on the said data using the machine learning method and comparison of the periodicity of the received computer mouse interrupt signal with the said statistical model.

15 [00067] All details of the implementation of data collection on the periodicity of the computer mouse interrupt signal, as well as the training of the statistical model based on the data obtained, are described above.

[00068] In any domain, consumer nodes, servers, trunk connections, etc. are considered “local” for this domain, while these elements at another domain are
20 considered as “remote”.

[00069] a remote access server, configured to receive a signal from a computer mouse from a remote access client;

[00070] a remote access client, configured to transmit a signal concerning the computer mouse interrupt to a remote access server;

25 [00071] computer mouse;

[00072] browser configured to load a script for collecting and transmitting data on the periodicity of computer mouse interrupt signal on a user’s device.

[00073] The person skilled in the art can easily implement other variations of the technology from the discussed description disclosed herein. This application is
30 intended to cover any embodiments of the technology, and including such deviations

from the present technology, which appear within the limits of known or common practice in the prior art. It is assumed that the description and examples are considered only as exemplary, with the summary and scope of the present technology, indicated by the technical solution claims.

- 5 **[00074]** It should be taken into account that the present disclosure is not limited to the precise structures that have been described above and illustrated in the accompanying drawings, and that various modifications and changes can be made without shifting away from its application field. It is assumed that the scope of the technical solution is limited only by the claims attached.

CLAIMS

1. A method of remote connection detection when working on web resource pages, the method comprising:
 - collecting data on a periodicity of computer mouse interrupt signals and training a statistical model using a machine learning method on the basis of the data collected, wherein the computer mouse interrupt signals are generated by corresponding programs that are triggered by mouse movement, and wherein the trained statistical model is representative of a typical periodicity of the computer mouse interrupt signals associated with a legitimate user;
 - receiving computer mouse interrupt signals;
 - comparing, using the trained statistical model, a current periodicity of the received computer mouse interrupt signals with the typical periodicity of the computer mouse interrupt signals associated with the legitimate user; and
 - in case of a deviation in the current periodicity of the received computer mouse interrupt signals identified based on the comparison with the typical periodicity, notifying an owner of the protected web resource of a presence of a remote connection by a visitor of web resource for subsequent response from the owner's side.
2. The method of claim 1, wherein the data on the periodicity of the computer mouse interrupt signals are the median and the dispersion of the time measurements set distribution (in ms) between adjacent calls of the computer mouse interrupt signals.
3. The method of claim 1, wherein, for training the statistical model based on the data collected, the machine learning method such as a k-nearby neighbours method or linear regression is used.

4. The method of claim 1, wherein, for training the statistical model based on the data collected, approximating functions for calculating the parameters necessary for detecting the use of remote access means are used.
5. A system for remote connection detection when working on web resource pages, the system comprising:
- a server configured to collect data on a periodicity of computer mouse interrupt signals, train a statistical model based on the collected data using a machine learning method, wherein the computer mouse interrupt signals are generated by corresponding programs that are triggered by mouse movement, and wherein the trained statistical model is representative of a typical periodicity of the computer mouse interrupt signals associated with a legitimate user, the server being further configured to compare, using the trained statistical model, a current periodicity of received computer mouse interrupt signals with the typical periodicity of the computer mouse interrupt signals associated with the legitimate user;
 - a remote access server, configured to receive a signal from a computer mouse from a remote access client;
 - a remote access client, configured to transmit a signal about the computer mouse interrupt to a remote access server;
 - computer mouse;
 - browser configured to load a script for collecting and transmitting data on the periodicity of computer mouse interrupt signals on a user's device.
6. A server for remote connection detection when working on web resource pages, the server being configured to:
- collect data on a periodicity of computer mouse interrupt signals, wherein the computer mouse interrupt signals are generated by corresponding programs that are triggered by mouse movement;

- train a statistical model based on the collected data using a machine learning method, wherein the trained statistical model is representative of a typical periodicity of the computer mouse interrupt signals associated with a legitimate user;
- 5 • receive computer mouse interrupt signals;
- compare, using the trained statistical model, a current periodicity of the received computer mouse interrupt signals with the typical periodicity of the computer mouse interrupt signals associated with the legitimate user; and
- 10 • in case of a deviation in the current periodicity of the received computer mouse interrupt signals identified based on the comparison with the typical periodicity, notify an owner of the protected web resource of a presence of a remote connection by a visitor of web resource for subsequent response from the owner's side.

15