

MULTI-FRAME CYBER SECURITY ANALYSIS DEVICE AND RELATED COMPUTER PROGRAM PRODUCT FOR GENERATING MULTIPLE ASSOCIATED DATA FRAMES

BACKGROUND

[0001] The disclosure generally relates to a cyber breach inspection technology and, more particularly, to cyber security analysis device and related computer program product for generating multiple associated data frames.

[0002] As various internet applications become more common, cyber breach events happen one after the other everywhere. General antivirus software installed in computers can detect and block common viruses; however, they cannot effectively prevent or detect cyber intrusions conducted by hackers. For example, a cyber attacking approach that has become increasingly prevalent in recent years, known as the advanced persistent threat (APT), is a prolonged, advanced, and all-round attack to a specific enterprise or organization. Usually, this kind of cyberattack is a targeted attack sponsored by a specific country or organizations, with a primary purpose of stealing specific information, cryptocurrency, the privacy of specific person, or the like. However, it is difficult for normal security protection software to detect such kind of cyberattack.

[0003] Due to the diversity of cyberattack approaches, the current technology cannot yet solely rely on computer programs to make an accurate judgement. In practice, in order to inspect whether a specific environment has been attacked by the aforementioned APT or other types of cyberattack approaches, it is necessary to rely on experienced professional cyber security analysts to repeatedly conduct data interpretation, data filtering, and cross-comparison on numerous history records of computer activities with respect to the inspected environment so as to make a judgement. However, the aforementioned inspection approach highly relies on the practical experience of the cyber security analysts, and moreover, the cyber security analyst has to use different searching conditions to filter data from numerous history records of computer activities, and to make record of each filtering result by himself/herself for conducting cross-comparison. Thus, the whole determining process is considerably labor and time consuming, and it generally takes several working days to conclude a preliminary judgement.

SUMMARY

[0004] In view of the foregoing, it may be appreciated that a substantial need exists for increasing the determining efficiency and accuracy in diagnosing whether or not a particular environment is breached by cyber attacks.

[0005] An example embodiment of a multi-frame cyber security analysis device for diagnosing whether a target network system is breached by hackers is disclosed, comprising: a display device; an input device, arranged to operably receive operation commands issued by a user; a non-volatile storage circuit, arranged to operably store a database and an associated data frame generating program, wherein the database is stored with device activities records of multiple types related to multiple computing devices in the target network system; and a control circuit, coupled with the display device, the input device, and the non-volatile storage circuit, and arranged to operably execute the associated data frame generating program, so as to conduct data frame generating operation according to the device activities records of multiple types stored in the database to generate multiple associated data frames related to the target network system and to display contents of the multiple associated data frames at the same time; wherein the multiple associated data frames comprise a navigator frame, a first global data frame, and a local data frame.

[0006] Another example embodiment of a non-transitory computer program product is disclosed. The non-transitory computer program product is stored in a non-volatile storage circuit of a multi-frame cyber security analysis device and enables the multi-frame cyber security analysis device to conduct a data frame generating operation according to device activities records of multiple types stored in a database, so as to generate multiple associated data frames related to a target network system, and to display contents of the multiple associated data frames at the same time, wherein the multiple associated data frames comprise a navigator frame, a first global data frame, and a local data frame.

[0007] Both the foregoing general description and the following detailed description are examples and explanatory only, and are not restrictive of the invention as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] FIG. 1 shows a simplified functional block diagram of a cyber breach diagnostics system according to one embodiment of the present disclosure.

[0009] FIG. 2 shows a simplified schematic diagram of functional modules of a device activities reporting program installed in respective computing devices in FIG. 1 according to

one embodiment of the present disclosure.

[0010] FIG. 3 shows a simplified schematic diagram of functional modules of an associated data frame generating program installed in a multi-frame cyber security analysis device in FIG. 1 according to one embodiment of the present disclosure.

[0011] FIG. 4 shows a simplified flowchart of a method for diagnosing whether a target network system is breached by hackers according to one embodiment of the present disclosure.

[0012] FIG. 5 shows a simplified schematic diagram of a multi-frame screen displayed by a display device in FIG. 1 according to one embodiment of the present disclosure.

[0013] FIGS. 6~7 collectively show simplified flowcharts of a method for generating multiple associated data frames according to one embodiment of the present disclosure.

[0014] FIGS. 8~12 show simplified schematic diagrams of partial contents in the multiple-frame screens according to different embodiments of the present disclosure.

[0015] FIG. 13 shows a simplified functional block diagram of the cyber breach diagnostics system according to another embodiment of the present disclosure.

DETAILED DESCRIPTION

[0016] Reference is made in detail to embodiments of the invention, which are illustrated in the accompanying drawings. The same reference numbers may be used throughout the drawings to refer to the same or like parts, components, or operations.

[0017] FIG. 1 shows a simplified functional block diagram of a cyber breach diagnostics system 100 according to one embodiment of the present disclosure. The cyber breach diagnostics system 100 is utilized for diagnosing whether a target network system 102 is breached by hackers. As shown in FIG. 1, the target network system 102 comprises multiple computing devices (e.g., exemplary computing devices 111~115 shown in FIG. 1). Please note that the quantity of the computing devices shown in FIG. 1 is merely for the illustrative purpose, and does not intend to limit the quantity of the computing devices in the target network system 102 to any particular number.

[0018] The term “computing device” used throughout the description and the claims refers to various electronic equipment capable of executing specific operating system (e.g., Windows, Linux, macOS, Android, Chrome OS, HarmonyOS, or the like) to operate while supporting appropriate data communication protocols, such as a desktop computer, a laptop computer, a tablet computer, a server, a NAS (network attached storage), a smart television, a smart phone, a smart speaker, or the like. The aforementioned data communication protocols may be various

wired transmission protocols or wireless data communication protocols, such as TCP/IP (transmission control protocol/internet protocol) communication protocols, UDP (user datagram protocol) communication protocol, USB (universal serial bus) communication protocols, IEEE 802.11 series communication protocols, Bluetooth series communication protocols, or the like.

[0019] In practical applications, the target network system 102 may be an internal network system of enterprises, schools, research institutes, or organizations of various scales, and therefore the quantity of the computing devices of the target network system 102 may be single-digit numbers, dozens, hundreds, or even more than one thousand. In addition, the multiple computing devices of the target network system 102 may be located in a same geographical region, or may be located in different geographical regions (e.g., different cities or countries).

[0020] Each computing device in the target network system 102 may directly or indirectly communicate various data with another one or more than one computing devices through appropriate data transmission mechanisms (e.g., an intranet or data transmission cables within the target network system 102). In operations, a part of the computing devices in the target network system 102 may employ wired data transmission approach to conduct data communications, while another part of the computing devices may employ wired data transmission approach to conduct data communications. In other words, different computing devices may employ different data transmission approaches.

[0021] In the embodiment of FIG.1, the cyber breach diagnostics system 100 comprises multiple device activities reporting programs 120, an activity records collection device 130, and a multi-frame cyber security analysis device 140.

[0022] The multiple device activities reporting programs 120 in the cyber breach diagnostics system 100 are respectively stored and installed in the aforementioned multiple computing devices 111~115 of the target network system 102. The multiple device activities reporting programs 120 are arranged to operably generate multiple suspicious activities records and multiple time stamps related to the multiple computing devices 111~115, and to operably create multiple attribute tags respectively corresponding to the multiple suspicious activities records.

[0023] The activity records collection device 130 comprises a communication circuit 131, a processing circuit 133, and a storage circuit 135. The communication circuit 131 is coupled with the target network system 102, and arranged to operably conduct data communications with the aforementioned multiple computing devices 111~115 through appropriate network connections (e.g., an intranet of target network system 102 or the internet), so as to receive the

multiple suspicious activities records generated by the multiple device activities reporting programs 120, the corresponding multiple time stamps, and the corresponding multiple attribute tags. The processing circuit 133 is coupled with the communication circuit 131, and arranged to operably control operations of the communication circuit 131, and to operably process the received multiple suspicious activities records, multiple time stamps, and multiple attribute tags to generate a return data. The processing circuit 133 further utilizes the communication circuit 131 to transmit the return data to the multi-frame cyber security analysis device 140 through appropriate networks (e.g., the internet). The storage circuit 135 is coupled with the processing circuit 133, and arranged to operably store data or files required for operations of the activity records collection device 130.

[0024] In practical application, the aforementioned activity records collection device 130 may be installed within the building in which the target network system 102 resides, or may be installed in other location outside the building in which the target network system 102 resides.

[0025] As shown in FIG. 1, the multi-frame cyber security analysis device 140 comprises a display device 141, a communication circuit 143, an input device 145, a non-volatile storage circuit 147, and a control circuit 149. The display device 141 is utilized to display various data and images. The communication circuit 143 is arranged to operably receive the aforementioned return data through appropriate networks (e.g., the internet). The input device 145 is arranged to operably enable users of the multi-frame cyber security analysis device 140 (e.g., cyber security analysts) to conduct various manipulations on the multi-frame cyber security analysis device 140, such as inputting commands, modifying related analyzing parameters, adjusting related data comparison criteria, or adjusting the size, position, or contents of images displayed by the display device 141, or the like. The storage circuit 147 is arranged to operably store a database 152 and an associated data frame generating program 154, wherein the database 152 is utilized to store device activities records of multiple types related to the aforementioned multiple computing devices 111~115 in the target network system 102. The control circuit 149 is coupled with the display device 141, the communication circuit 143, the input device 145, and the storage circuit 147, and arranged to operably extract the multiple suspicious activities records related to the multiple computing devices 111~115 of the target network system 102, the corresponding multiple time stamps, and the corresponding multiple attribute tags from the return data received by the communication circuit 143. The control circuit 149 is further arranged to operably execute the associated data frame generating program 154 to conduct a data frame generating operation. In the data frame generating operation, the control circuit 149 generates multiple associated data frames related to the target

network system 102 according to the device activities records of multiple types stored in the database 152, and utilizes the display device 141 to display contents of the multiple associated data frames at the same time.

[0026] In addition, the exemplary malicious file providing device 160 of FIG. 1 denotes one of the phishing websites, zombie computers, network servers for spreading malicious program codes, or other device entities playing similar roles that may be employed by the hackers in breaching the target network system 102. In actual cyber breach events, the hackers may attempt to attack the target network system 102 by employing more than one malicious file providing devices.

[0027] In practice, each of the aforementioned communication circuit 131 and 143 may be realized with various wired transmission circuits, wireless transmission circuits, or a hybrid circuit integrating the aforementioned two communication mechanisms. The processing circuit 133 may be realized with one or more processor units. The storage circuit 135 and 147 may be realized with various non-volatile storage devices. The database 152 may be realized with various relational databases, or various non-relational databases. The database 152 and the associated data frame generating program 154 may be stored in a same storage medium in the storage circuit 147, or may be respectively stored in different storage mediums in the storage circuit 147. The display device 141 may be realized with a single screen or a single projection device capable of displaying images, or may be realized with a combination of multiple screens or a combination of multiple projection devices. The input device 145 may be realized with a keyboard, a mouse, a remote control, a touch screen, a touch panel, buttons, a voice-activated input device, a gesture sensing device, a circuit using other various command generating technologies, or a combination of the aforementioned devices. The control circuit 149 may be realized with a single processor module, a combination of multiple processor modules, a computer system, a server, or a cloud system. In addition, the aforementioned display device 141 and the input device 145 may be collectively integrated into a single touch screen or a combination of multiple touch screens.

[0028] Each of the aforementioned device activities reporting programs 120 stored in different computing devices of the target network system 102 may be realized with a computer program product formed by one or more functional modules. For example, FIG. 2 shows a simplified schematic diagram of functional modules of the device activities reporting program 120 installed in respective computing devices in FIG. 1 according to one embodiment of the present disclosure. In the embodiment of FIG. 2, the device activities reporting program 120 comprises a detection module 210, a property determining module 220, and a transmission

module 230.

[0029] In addition, the aforementioned associated data frame generating program 154 stored in the storage circuit 147 of the multi-frame cyber security analysis device 140 may be realized with a computer program product formed by one or more functional modules. For example, FIG. 3 shows a simplified schematic diagram of functional modules of the associated data frame generating program 154 installed in the multi-frame cyber security analysis device 140 according to one embodiment of the present disclosure. In the embodiment of FIG. 3, the associated data frame generating program 154 comprises an accessing module 310, a navigator frame generating module 320, a global data frame generating module 330, a local data frame generating module 340, and a frame association control module 350.

[0030] The operations of the cyber breach diagnostics system 100 will be further described below by reference to FIG. 4. FIG. 4 shows a simplified flowchart of a method for diagnosing whether a target network system 102 is breached by hackers according to one embodiment of the present disclosure.

[0031] In the flowchart of FIG. 4, operations within a column under the name of a specific device are operations to be performed by the specific device. For example, operations within a column under the label “computing device” are operations to be performed by respective computing devices 111~115 in the target network system 102; operations within a column under the label “activity records collection device” are operations to be performed by the activity records collection device 130; and operations within a column under the label “multi-frame cyber security analysis device” are operations to be performed by the multi-frame cyber security analysis device 140.

[0032] During the routine operations of the aforementioned target network system 102, respective computing devices execute the device activities reporting programs 120 installed therein to conduct the operations 402 through 406 in FIG. 4.

[0033] In the operation 402, the detection module 210 of the device activities reporting program 120 detects and collects the suspicious activities records and the time stamps related to the computing device in which it is installed. For the convenience of description, the computing device 111 is taken as an example for description in the following.

[0034] The device activities reporting program 120 installed in the computing device 111 may utilize the detection module 210 to access and analyze the contents of specific non-volatile data in the computing device 111, such as the system logs, the processes which are automatically executed after boot up, the file execution records, and/or the meta data of files of specific types or the like, in the operation 402.

[0035] For example, in the case that the operating system of the computing device 111 is the Windows system, the detection module 210 may access and analyze the Windows Event Logs, the Autorun Registry Schedule Jobs, the Prefetch cache, the Shimcache and/or the Amcache, and/or the meta data of PE files (portable executable files) of .exe/.dll/.sys formats, or the like stored in the computing device 111.

[0036] For another example, in the case that the operating system of the computing device 111 is the Linux system, the detection module 210 may access and analyze the log items under “/var/log/” directory, the Systemd, the SysV init script, the crontab, the Upstart, the dynamic web pages of .php or .jsp format, the shell scripts, the sensitive files, the command histories, the syslog, and/or the meta data of the ELF files (executable and linkable format files) of .so/.ko formats, or the like stored in the computing device 111.

[0037] For yet another example, in the case that the operating system of the computing device 111 is the macOS system, the detection module 210 may access and analyze the log items under “/var/log/” directory, the records under “/Library/LaunchAgents/” directory, the records under “/Library/LaunchDaemons/” directory, the shell scripts, the command histories, and/or the meta data of the Mach-O files (Mach object files), or the like stored in the computing device 111.

[0038] In addition to the aforementioned non-volatile data, the detection module 210 may detect and analyze the contents of specific volatile data of the computing device 111 in the operation 402, such as the current contents of the memory of the computing device 111 and/or the network activities of the computing device 111. For example, the detection module 210 may utilize a network connection inquiry command “netstat” to inquire the status of the computing device 111 regarding the connection with external networks, and may utilize various approaches to detect the IP addresses accessed by the computing device 111 as well as the operating situations of the network ports of the computing device 111.

[0039] In operations, the detection module 210 may adopt various filtering and determination algorithms to conduct a preliminary analysis on the contents of the aforementioned specific non-volatile data and/or volatile data related to the computing device 111 so as to filter activities records possibly associated with cyber breach events from numerous activities records of the computing device 111 to be suspicious activities records, thereby reducing the data volume to be processed or analyzed by the activity records collection device 130 and the multi-frame cyber security analysis device 140 in the subsequent stage.

[0040] In practical applications, the suspicious activities records determined by the detection module 210 may comprise historical records of various types, such as file execution

activities, file creation activities, file editing activities, networking activities, keystroke logging activities, password stealing activities, credential dumping activities, code injection activities, code manipulation activities, and/or executable code accessing activities, or the like related to the computing device 111.

[0041] The substantial physical meanings of the suspicious activities records may be appreciated from their names, and the detailed definitions of respective suspicious activities records are determined by the record detection rules of the detection module 210. Under different detection rules, the same suspicious activities record may have slightly different specific definitions.

[0042] In addition, when the detection module 210 determines that a specific activities record is a suspicious activities record, the detection module 210 would also record a time stamp in the computing device 111 with respect to the specific activities record to be a corresponding time stamp of the specific suspicious activities record.

[0043] In practice, the detection module 210 of the device activities reporting program 120 may conduct, in real time, the aforementioned operation 402 during the operation of the computing device 111, or may intermittently or periodically conduct the aforementioned operation 402.

[0044] In the operation 404, the property determining module 220 of the device activities reporting program 120 may create the attribute tags corresponding to the suspicious activities records according to the analysis results of the aforementioned detection module 210 with respect to the suspicious activities records.

[0045] For example, for the suspicious activities records been determined by the detection module 210 as being related to the malicious program family used by known APT attacks, the property determining module 220 may set a corresponding tag “APT Malware” for such suspicious activities records.

[0046] For another example, for the suspicious activities records been determined by the detection module 210 as being related to the programs which are automatically executed after boot up, the property determining module 220 may set a corresponding tag “Autorun” for such suspicious activities records.

[0047] For yet another example, for the suspicious activities records been determined by the detection module 210 as being related to the programs involving in networking activities, the property determining module 220 may set a corresponding tag “Networking” for such suspicious activities records.

[0048] For yet another example, for the suspicious activities records been determined by the

detection module 210 as being related to the programs or memory contents having the keystroke logging functionality, the property determining module 220 may set a corresponding tag “Keystroke Logging” for such suspicious activities records.

[0049] For yet another example, for the suspicious activities records been determined by the detection module 210 as being related to the programs having functionalities of stealing password or credentials, the property determining module 220 may set a corresponding tag “Password Stealer” for such suspicious activities records.

[0050] For yet another example, for the suspicious activities records been determined by the detection module 210 as being related to the files having hidden attributes, the property determining module 220 may set a corresponding tag “Hidden Files” for such suspicious activities records.

[0051] For yet another example, for the suspicious activities records been determined by the detection module 210 as being related to the executable codes in memory blocks, the property determining module 220 may set a corresponding tag “Executable Code” for such suspicious activities records.

[0052] For yet another example, for the suspicious activities records been determined by the detection module 210 as related to suspicious code injections or shellcodes, the property determining module 220 may set a corresponding tag “Code Manipulation” for such suspicious activities records.

[0053] For yet another example, for the suspicious activities records been determined by the detection module 210 as being related to the memory contents having characteristics of known malicious programs, the property determining module 220 may set a corresponding tag “Malware” for such suspicious activities records.

[0054] For yet another example, for the suspicious activities records been determined by the detection module 210 as being related to the memory contents having functionalities of stealing passwords or credentials, the property determining module 220 may set a corresponding tag “Access Credentials” for such suspicious activities records.

[0055] After the property determining module 220 sets the attribute tags, different suspicious activities records may have the same attribute tag, or may have different attribute tags. In addition, the property determining module 220 may set multiple different attribute tags for the same suspicious activities record, and thus different suspicious activities records may have different quantities of attribute tags.

[0056] In the operation 406, the transmission module 230 of the device activities reporting program 120 may transmit the suspicious activities records related to the computing device 111,

the corresponding time stamps, and the corresponding attribute tags to the activity records collection device 130 through appropriate data transmission approaches.

[0057] The device activities reporting program 120 in each of other computing devices 112~115 may individually conduct the operations 402~406 by adopting the aforementioned method, so as to transmit the suspicious activities records of the related computing device, the corresponding time stamps, and the corresponding attribute tags to the activity records collection device 130.

[0058] In addition, the multiple device activities reporting programs 120 in the aforementioned multiple computing devices 111~115 may simultaneously perform the aforementioned operations 402~406 in a same predetermined time period, or may independently perform the aforementioned operations 402~406 in different time periods.

[0059] As can be appreciated from the foregoing descriptions, the multiple device activities reporting programs 120 in the aforementioned computing devices 111~115 would respectively generate multiple suspicious activities records and multiple time stamps related to the computing devices 111~115, and create multiple attribute tags corresponding to the multiple suspicious activities records.

[0060] In the operation 408, the communication circuit 131 of the activity records collection device 130 may receive the multiple suspicious activities records, the corresponding multiple time stamps, and the corresponding multiple attribute tags transmitted from the multiple computing devices 111~115 of the target network system 102 through appropriate network connections (e.g., an intranet of the target network system 102 or the internet).

[0061] In the operation 410, the processing circuit 133 of the activity records collection device 130 processes the received multiple suspicious activities records, the corresponding multiple time stamps, and the corresponding multiple attribute tags so as to generate a return data. For example, the processing circuit 133 may conduct various processes, such as data encapsulation, compression, encryption, electronic signature, partitioning, or the like, on the received multiple suspicious activities records, the corresponding multiple time stamps, and the corresponding multiple attribute tags so as to generate a return data in appropriate formats.

[0062] In the operation 412, the processing circuit 133 utilizes the communication circuit 131 to transmit the return data to the multi-frame cyber security analysis device 140 through an appropriate network (e.g., the internet).

[0063] In the operation 414, the communication circuit 143 of the multi-frame cyber security analysis device 140 may receive the return data generated by the activity records collection device 130 through an appropriate network (e.g., the internet).

[0064] In the operation 416, the control circuit 149 of the multi-frame cyber security analysis device 140 processes the received return data so as to acquire the multiple suspicious activities records related to the target network system 102, the corresponding multiple time stamps, and the corresponding multiple attribute tags from the return data. For example, the control circuit 149 may conduct various processes, such as combination, decompression, decryption, electronic signature verification, or the like, on the return data to extract the aforementioned activities records, time stamps, and attribute tags from the return data.

[0065] In the operation 418, the control circuit 149 executes the associated data frame generating program 154 stored in the storage circuit 147 to conduct a data frame generating operation according to the aforementioned multiple suspicious activities records, the corresponding multiple time stamps, and the corresponding multiple attribute tags so as to generate and display a multi-frame screen which comprises multiple associated data frames at the same time.

[0066] Please refer to FIG. 5, which shows a simplified schematic diagram of a multi-frame screen 500 displayed by the display device 141 of the multi-frame cyber security analysis device 140 according to one embodiment of the present disclosure.

[0067] As shown in FIG. 5, the multi-frame screen 500 displayed by the display device 141 comprises multiple data frames (e.g., the exemplary data frames 510~540 shown in FIG. 5). Each of the data frames 510~540 in the multi-frame screen 500 may be utilized to display text information or graphic information of various types, such as device topology diagrams, device interaction relationship diagrams, statistic graphs, analysis graphs, data sheets, menus, document or file lists, or the like. Contents of the aforementioned data frames 510~540 may be utilized as judgement basis for the cyber security analysts in diagnosing whether the target network system 102 is breached by hackers or not.

[0068] In the embodiment of FIG. 5, the data frames 510~530 are utilized to represent data contents generated by the multi-frame cyber security analysis device 140 after executing the associated data frame generating program 154, and the data frames 510~530 respectively belong to three different frame types. Specifically, the data frame 510 is an associated data frame utilized for displaying multiple filtering conditions, and is hereinafter referred to as a navigator frame 510; the data frame 520 is an associated data frame utilized for displaying specific global property data related to a portion of or all devices in the target network system 102, and is hereinafter referred to as a first global data frame 520; while the data frame 530 is an associated data frame utilized for displaying a specific data group corresponding to one of the aforementioned multiple computing devices 111~115, and is hereinafter referred to as a

local data frame 530.

[0069] In addition, the data frame 540 is a frame of other types, and the contents displayed in the data frame 540 would not associate with the change of the contents in the aforementioned navigator frame 510, the first global data frame 520, or the local data frame 530.

[0070] During conducting the diagnosing process, the cyber security analyst may conduct various manipulations through the input device 145 to increase or decrease the quantity of data frames of various types, to adjust the size or position of respective data frames, to select objects in respective data frames, to modify related analyzing parameters, to issue various commands, or the like.

[0071] As can be appreciated from the foregoing descriptions, the multiple computing devices 111~115 in the target network system 102 may transmit the related suspicious activities records, the time stamps, and the multiple attribute tags to the activity records collection device 130, then the activity records collection device 130 accordingly generates the return data and transmits to the multi-frame cyber security analysis device 140. This approach is beneficial in reducing outbound networking bandwidth requirement of the target network system 102, and is also beneficial in enhancing the security of data transmission between the activity records collection device 130 and the multi-frame cyber security analysis device 140.

[0072] In the associated data frame generating program 154, the accessing module 310 is an agent utilized by other modules to access the database 152. When other modules need to access the multiple suspicious activities records, the corresponding multiple time stamps, and the corresponding multiple attribute tags, other modules may instruct the accessing module 310 to utilize the control circuit 149 to access the data stored in the database 152.

[0073] In addition, the accessing module 310 may identify multiple suspicious events related to the target network system 102 as well as multiple time records respectively corresponding to the multiple suspicious events based on the data stored in the database 152.

[0074] For the accessing module 310, the aforementioned multiple suspicious activities records, the corresponding multiple time stamps, and the corresponding multiple attribute tags are digital evidences that can be utilized for analyzing whether specific events have occurred in the target network system 102. The accessing module 310 may conduct a cross-comparison and an event correlation analysis on the aforementioned multiple suspicious activities records, the corresponding multiple time stamps, and the corresponding multiple attribute tags by adopting various rule matching algorithms or artificial intelligence algorithms so as to identify multiple suspicious events that are possibly associated with cyber breach activities in the target network system 102, and to identify multiple time records respectively corresponding to the

aforementioned multiple suspicious events.

[0075] For example, the accessing module 310 may conduct various cross-comparisons and event correlation analyses based on multiple suspicious activities records related to a specific computing device, so as to find out one or more suspicious events having sufficiently affirmative digital evidences capable of proving that the one or more suspicious events took place in the specific computing device. In addition, the accessing module 310 may also conduct various cross-comparisons and event correlation analyses on multiple suspicious activities records with respect to two different computing devices, so as to find out one or more suspicious events having sufficiently affirmative digital evidences capable of proving that the one or more suspicious events took place between the two computing devices.

[0076] Moreover, the accessing module 310 may also identify a start time or an end time for each suspicious event according to the aforementioned multiple time stamps, and utilize the identified start time or end time as a corresponding time record of the suspicious event.

[0077] For simplicity of illustration, the suspicious events took place within respective computing devices are hereinafter referred to as device internal events, while the suspicious events took place between two different computing devices are hereinafter referred to as device interaction events.

[0078] The types and quantity of the device internal events identified by the accessing module 310 based on the aforementioned digital evidences (i.e., the suspicious activities records, the time stamps, and the attribute tags) are determined by the actual situation of the target network system 102. Similarly, the types and quantity of the device interaction events identified by the accessing module 310 based on the aforementioned digital evidences are also determined by the actual situation of the target network system 102.

[0079] If the device internal events or the device interaction events identified by the accessing module 310 have too many types, it would easily render the contents in the resulting multiple associated data frames 510~530 become too packed or messy, and thus cause the cyber security analysts to be interfered by noisy information, thereby adversely affecting the interpreting and analyzing efficiency of the cyber security analysts.

[0080] In order to decrease the problems described above, the accessing module 310 may configure a corresponding first upper limit for the quantity of types of the device internal events, and configure a corresponding second upper limit for the quantity of types of the device interaction events. The aforementioned first upper limit and second upper limit may be the same with each other or may be different from each other

[0081] In operations, the accessing module 310 may select certain types of the device

internal events and certain types of the device interaction events to be displayed in the multiple associated data frames 510~530 according to the importance of the event type, rareness of the event type, sensitivity of the event type, event quantity, and/or other considering factors.

[0082] For example, the accessing module 310 may limit the quantity of types of the device internal events that can be displayed in the multiple associated data frames 510~530 to at most eight types, which are file creation events, file access events, registry creation events, schedule task events, file execution events, memory module detection events, memory process creation events, and privileges escalation events. In the meantime, the accessing module 310 may limit the quantity of types of the device interaction events that can be displayed in the multiple associated data frames 510~530 to at most six types, which are remote logon events, brute-force logon events, attempt logon events, remote access events, file moving events, and network download events. In other words, the aforementioned first upper limit is eight while the second upper limit is six in this embodiment.

[0083] In another embodiment, the accessing module 310 may limit the quantity of types of the device internal events that can be displayed in the multiple associated data frames 510~530 to at most three types, which are the aforementioned file creation events, file execution events, and memory process creation events. In the meantime, the accessing module 310 may limit the quantity of types of the device interaction events that can be displayed in the multiple associated data frames 510~530 to at most four types, which are the aforementioned remote logon events, remote access events, file moving events, and network download events. In other words, the aforementioned first upper limit is three while the second upper limit is four in this embodiment.

[0084] The substantial physical meanings of the respective events may be appreciated from their names, and the detailed definitions of respective events are determined by the analysis rules of the event correlation analysis conducted by the accessing module 310. Under different analysis rules, the same event type may have slightly different specific definitions.

[0085] In practical applications, the accessing module 310 may dynamically adjust the aforementioned first upper limit and second upper limit according to the display space of the multiple associated data frames 510~530, or may flexibly adjust the aforementioned first upper limit and second upper limit in view of other design considerations.

[0086] The accessing module 310 may store the identified suspicious events and the corresponding time records in the database 152, so that these data can be utilized as one of the reference basis by other modules in generating related frames.

[0087] The data frame generating operation conducted by the multi-frame cyber security

analysis device 140 will be further described in the following by reference to FIG. 6 through FIG. 7. FIGS. 6~7 collectively show simplified flowcharts of a method for generating multiple associated data frames according to one embodiment of the present disclosure. In the flowcharts of FIG. 6 and FIG. 7, operations within a column under the name of a specific module are operations to be performed by the specific module. For example, operations within a column under the label “navigator frame generating module” are operations to be performed by the navigator frame generating module 320 of the associated data frame generating program 154; operations within a column under the label “global data frame generating module” are operations to be performed by the global data frame generating module 330; operations within a column under the label “local data frame generating module” are operations to be performed by the local data frame generating module 340; and operations within a column under the label “frame association control module” are operations to be performed by the frame association control module 350.

[0088] In the operation 602, the navigator frame generating module 320 generates multiple candidate objects respectively corresponding to multiple filtering conditions, so as to render different candidate objects to be respectively corresponding to different filtering conditions. The aforementioned multiple filtering conditions are various conditions that may be employed to conduct searching, filtering, or classifying on numerous data stored in the database 152, such as dates, time ranges, keywords, device risk types and risk levels, device groups, network segments in which the device resides (IP address ranges), device connection types, device interaction types, or the like.

[0089] In practice, the navigator frame generating module 320 may utilize various graphs, images, or texts to represent respective candidate objects, and different candidate objects may have the same visual representation with each other or may have different visual representations from each other.

[0090] In the embodiment of FIG. 5, for example, the navigator frame generating module 320 utilizes selectable date grids to be the visual representation of the multiple candidate objects (e.g., the exemplary candidate objects 511, 513, and 515 in FIG. 5). In this situation, different candidate objects respectively denote different dates. For example, the candidate object 511 corresponds to a first date, the candidate object 513 corresponds to a second date, and the candidate object 515 corresponds to a third date.

[0091] In the operation 604, the navigator frame generating module 320 establishes the navigator frame 510 comprising the aforementioned multiple candidate objects. In practice, the navigator frame generating module 320 may arrange or combine the aforementioned

multiple candidate objects in various appropriate ways, so that it would be more convenient for the cyber security analyst to differentiate different candidate objects.

[0092] In the embodiment of FIG. 5, for example, the navigator frame generating module 320 may arrange the aforementioned multiple candidate objects in a form of a calendar menu and configure the calendar menu to be the navigator frame 510.

[0093] In the operation 606, the global data frame generating module 330 generates multiple global property data related to a portion of or all devices in the target network system 102 according to the data stored in the database 152, so as to render different global property data to be respectively corresponding to different filtering conditions. In practice, the global data frame generating module 330 may organize various data stored in the database 152 into the multiple global property data corresponding to the aforementioned filtering conditions. For example, the multiple global property data may be network topology data of the target network system 102, network traffic rankings of all computing devices, data throughput rankings of all computing devices, malicious IP addresses accessed by all computing devices, lists of all malicious programs found in the target network system 102, lists of abnormal events founded in all computing devices in the target network system 102, historical records of executed abnormal instructions founded in all computing devices in the target network system 102, device activity relationship diagrams with respect to the target network system 102, suspicious events sequence diagrams with respect to the target network system 102, statistic graphs of computing device activities in the target network system 102, statistic graphs of the suspicious events in the target network system 102, or the like.

[0094] In addition, the filtering conditions configured by the navigator frame generating module 320 may have a one-to-one mapping relationship or a one-to-many mapping relationship with the global property data generated by the global data frame generating module 330. In one embodiment, the global data frame generating module 330 generates a corresponding global property data with respect to each filtering condition. In another embodiment, the global data frame generating module 330 generates global property data of two or more than two types with respect to each filtering condition. The global data frame generating module 330 may store the resulting multiple global property data in the database 152, so that the multiple global property data can be utilized in the subsequent operation period.

[0095] In the embodiment of FIG. 5, for example, the global data frame generating module 330 may establish multiple device activity relationship diagrams corresponding to a portion of or all devices in the target network system 102 according to the data stored in the database 152, while the aforementioned multiple device activity relationship diagrams respectively

correspond to different dates. For example, the aforementioned multiple device activity relationship diagrams may comprise a first device activity relationship diagram corresponding to the first date denoted by the candidate object 511 in the navigator frame 510, a second device activity relationship diagram corresponding to the second date denoted by the candidate object 513 in the navigator frame 510, and a third device activity relationship diagram corresponding to the third date denoted by the candidate object 515 in the navigator frame 510.

[0096] In the operation 608, the global data frame generating module 330 selects one of the multiple global property data to be a first target global property data. In practice, the global data frame generating module 330 may select a global property data corresponding to the filtering condition denoted by the selected candidate object in the navigator frame 510 to be the first target global property data. In the case that none of the candidate objects in the navigator frame 510 is selected, the global data frame generating module 330 may select a predetermined global property data corresponding to the type of the filtering conditions represented in the navigator frame 510 to be the first target global property data.

[0097] For example, if the currently selected candidate object in the navigator frame 510 is the candidate object 511, then the global data frame generating module 330 may select the first device activity relationship diagram corresponding to the first date denoted by the candidate object 511 to be the first target global property data.

[0098] In the operation 610, the global data frame generating module 330 establishes the first global data frame 520 comprising the first target global property data. In practice, the global data frame generating module 330 may simply configure the selected first target global property data as the first global data frame 520. Alternatively, the global data frame generating module 330 may combine the first target global property data together with other data and/or options to form the first global data frame 520.

[0099] In the embodiment of FIG. 5, for example, the global data frame generating module 330 may configure the first device activity relationship diagram corresponding to the first date as the first global data frame 520.

[0100] In the operation 612, the global data frame generating module 330 utilizes multiple main visual objects to respectively denote a portion of or all devices in the target network system 102 in the aforementioned first target global property data. In practice, the global data frame generating module 330 may utilize various graphs, images, or text boxes to represent the respective main visual objects, and different main visual objects may have the same visual representation with each other or may have different visual representations from each other.

[0101] In the embodiment of FIG. 5, for example, the global data frame generating module

330 utilizes a circular graph combined with brief descriptive texts to be the visual representation of the exemplary main visual objects 521, 523, and 525, and utilizes the main visual objects 521, 523, and 525 to represent different computing devices in the target network system 102 in the first device activity relationship diagram displayed in the first global data frame 520. For the convenience of description, it is assumed hereinafter that the main visual objects 521, 523, and 525 respectively correspond to three computing devices 111, 112, and 113 involved in the suspicious events in the target network system 102.

[0102] As shown in FIG. 5, the global data frame generating module 330 may respectively place the main visual objects 521, 523, and 525 at appropriate positions within the first global data frame 520 according to the representation of the first device activity relationship diagram.

[0103] Then, the associated data frame generating program 154 performs the operation 702 in FIG. 7.

[0104] In the operation 702, the local data frame generating module 340 generates multiple data groups respectively corresponding to the multiple computing devices 111~115 in the target network system 102 according to the data stored in the database 152. In practice, the local data frame generating module 340 may search the database 152 for device-specific information related to a specific computing device, and utilize the search results to be a data group corresponding to the specific computing device. The aforementioned device-specific information related to the specific computing device may be local property data related to internal activities of the specific computing device. For example, the local property data may be a list of executable programs within the specific computing device, a master-slave relationship diagram of executed processes within the specific computing device, networking connection records of the specific computing device, a historical list of executed instructions within the specific computing device, a list of internal abnormal events of the specific computing device, a statistic graph of internal cyber security risks of the specific computing device, a statistic graph of internal abnormal dates of the specific computing device, a profile data of the user account of the specific computing device, general information of the software and hardware of the specific computing device, a relationship diagram of internal specific files of the specific computing device and other similar files, or the like.

[0105] For example, the local data frame generating module 340 may search the database 152 for the device-specific information related to the computing device 111 so as to establish a first data group corresponding to the computing device 111; search the database 152 for the device-specific information related to the computing device 112 so as to establish a second data group corresponding to the computing device 112; and search the database 152 for the device-

specific information related to the computing device 113 so as to establish a third data group corresponding to the computing device 113. For the convenience of description, it is assumed hereinafter that the aforementioned first data group is an execution sequence diagram of programs within the computing device 111, the second data group is an execution sequence diagram of programs within the computing device 112, and the third data group is an execution sequence diagram of programs within the computing device 113.

[0106] In the operation 704, the local data frame generating module 340 selects one of the multiple data groups to be a first target data group. In practice, the local data frame generating module 340 may select a data group corresponding to the computing device denoted by the selected main visual object in the first global data frame 520 to be the first target data group. In the case that none of main visual objects in the first global data frame 520 is selected, the local data frame generating module 340 may select a predetermined data group corresponding to the type of the filtering conditions represented in the navigator frame 510 to be the first target data group, or may select a predetermined data group corresponding to the global property data being displayed in the first global data frame 520 to be the first target data group.

[0107] For example, if the currently selected main visual object in the first global data frame 520 is the main visual object 521, then the local data frame generating module 340 may select the first data group corresponding to the computing device 111 to be the first target data group.

[0108] In the operation 706, the local data frame generating module 340 establishes the local data frame 530 comprising the first target data group. In practice, the local data frame generating module 340 may simply configure the selected first target data group as the local data frame 530. Alternatively, the local data frame generating module 340 may combine the first target data group together with other data and/or options so as to form the local data frame 530.

[0109] In the embodiment of FIG. 5, for example, the local data frame generating module 340 may configure the first data group corresponding to the computing device 111 to be the local data frame 530.

[0110] In the operation 708, the frame association control module 350 controls the display device 141 to display the aforementioned navigator frame 510, the first global data frame 520, and the local data frame 530 at the same time to form the scheme shown in FIG. 5.

[0111] In this way, the cyber security analysts may acquire data related to the target network system 102 in different aspects or different dimensions at the same time from the contents of the navigator frame 510, the first global data frame 520, and the local data frame 530, and may utilize these data to be the judgement basis for diagnosing whether the target network system

102 is breached by hackers.

[0112] During conducting the diagnosing process, the cyber security analysts may need to adjust the filtering conditions to conduct cross-comparison on results acquired from different filtering conditions. In this situation, the cyber security analysts may manipulate the input device 145 to issue relevant operation commands so as to modify the contents of the multi-frame screen 500.

[0113] While the cyber security analysts manipulate the multi-frame cyber security analysis device 140, the associated data frame generating program 154 continuously performs the operation 710 and the operation 712 in FIG. 7.

[0114] In the operation 710, the frame association control module 350 monitors whether the selected candidate object in the navigator frame 510 is changed. In practice, the frame association control module 350 may determine whether the selected candidate object in the navigator frame 510 is changed according to the manipulation by the cyber security analysts on the input device 145. If the frame association control module 350 determines that the selected candidate object in the navigator frame 510 does not change, then the frame association control module 350 continues to perform the operation 710. On the contrary, if the frame association control module 350 determines that the selected candidate object in the navigator frame 510 is changed, then the frame association control module 350 performs the operation 714.

[0115] In the operation 712, the frame association control module 350 monitors whether the selected main visual object in the first global data frame 520 is changed. Similarly, the frame association control module 350 may determine whether the selected main visual object in the first global data frame 520 is changed according to the manipulation by the cyber security analysts on the input device 145. If the frame association control module 350 determines that the selected main visual object in the first global data frame 520 does not change, then the frame association control module 350 continues to perform the operation 712. On the contrary, if the frame association control module 350 determines that the selected main visual object in the first global data frame 520 is changed, then the frame association control module 350 performs the operation 716.

[0116] In the operation 714, the frame association control module 350 instructs the global data frame generating module 330 to replace the global property data in the first global data frame 520. In practice, the frame association control module 350 may inform the global data frame generating module 330 of information of a newly selected candidate object in the navigator frame 510 such as an object identification data, an object code, an identification data

of a corresponding filtering condition, a condition code of a corresponding filtering condition, or the like, so that the global data frame generating module 330 can learn that which is the newly selected candidate object in navigator frame 510.

[0117] In this situation, the global data frame generating module 330 would perform the operation 614 in FIG. 6 to select the global property data corresponding to the newly selected candidate object in the navigator frame 510 to be the aforementioned first target global property data. Then, as shown in FIG. 6, the global data frame generating module 330 performs the aforementioned operations 610 and 612 to replace the contents of the first global data frame 520 with the global property data corresponding to the newly selected candidate object in the navigator frame 510. In other words, in this situation, the global data frame generating module 330 replaces the contents of the first global data frame 520 with the global property data matching the filtering condition corresponding to the newly selected candidate object. After that, the frame association control module 350 controls the display device 141 to display the updated contents of the first global data frame 520.

[0118] In some embodiments, when the frame association control module 350 determines that a selected candidate object in the navigator frame 510 is changed, the frame association control module 350 would not instruct the local data frame generating module 340 to replace the target data group currently displayed in the local data frame 530. That is, the frame association control module 350 would not request the local data frame generating module 340 to consequentially change the target data group in the local data frame 530 in association with a change in the selected candidate object in the navigator frame 510.

[0119] In other embodiments, when the frame association control module 350 determines that a selected candidate object in the navigator frame 510 is changed, the frame association control module 350 would instruct the local data frame generating module 340 to replace the target data group currently displayed in the local data frame 530. For example, the frame association control module 350 may instruct the local data frame generating module 340 to replace the target data group currently displayed in the local data frame 530 with a predetermined data group corresponding to the filtering condition denoted by the newly selected candidate object. In other words, the frame association control module 350 may request the local data frame generating module 340 to consequentially change the target data group in the local data frame 530 in association with a change in the selected candidate object in the navigator frame 510.

[0120] In the operation 716, the frame association control module 350 instructs the local data frame generating module 340 to replace the target data group being displayed in the local

data frame 530. In practice, the frame association control module 350 may inform the local data frame generating module 340 of information of the newly selected main visual object in the first global data frame 520, such as the object identification data, object code, or identification data of a corresponding computing device, hardware code of the corresponding computing device, or other information, so that the local data frame generating module 340 can learn which is the newly selected main visual object in the first global data frame 520.

[0121] In this situation, the local data frame generating module 340 would perform the operation 718 in FIG. 7 to select the local property data corresponding to the newly selected main visual object in the first global data frame 520 to be the aforementioned target data group.

[0122] Then, as shown in FIG. 7, the local data frame generating module 340 performs the aforementioned operation 706 so as to replace the contents of the local data frame 530 with the local property data corresponding to the newly selected main visual object in the first global data frame 520. In other words, in this situation, the local data frame generating module 340 would replace the contents of the local data frame 530 with the matching local property data of the computing device corresponding to the newly selected main visual object. After that, the frame association control module 350 controls the display device 141 to display the updated contents of the local data frame 530.

[0123] However, when the frame association control module 350 determines that the selected main visual object in the first global data frame 520 is changed, the frame association control module 350 does not instruct the navigator frame generating module 320 to change the contents of the navigator frame 510. That is, the frame association control module 350 does not request the navigator frame generating module 320 to consequentially change the contents of the multiple candidate objects in the navigator frame 510 in association with a change in the selected main visual object in the first global data frame 520.

[0124] As can be appreciated from the foregoing descriptions, for example, in the multi-frame screen 500 as shown in FIG. 5, the candidate object being currently selected in the navigator frame 510 is the candidate object 511, and the first target global property data being currently displayed in the first global data frame 520 is the first device activity relationship diagram corresponding to the first date denoted by the candidate object 511. In this situation, if the user selects the candidate object 513 in the navigator frame 510 through the input device 145, then the frame association control module 350 would perform the operation 714 to instruct the global data frame generating module 330 to replace the global property data in the first global data frame 520.

[0125] Then, the global data frame generating module 330 performs the operation 614

according to instructions of the frame association control module 350 to select the second device activity relationship diagram corresponding to the second date denoted by the newly selected candidate object 513 to be the first target global property data, and to replace the contents of the first global data frame 520 with the aforementioned second device activity relationship diagram corresponding to the second date. The frame association control module 350 performs the operation 708 to control the display device 141 to display the updated contents of the first global data frame 520, so that the contents of the multi-frame screen 500 are changed to be the scheme as shown in FIG. 8.

[0126] In the embodiment of FIG. 8, in this situation, the frame association control module 350 would not instruct the local data frame generating module 340 to replace the target data group being currently displayed in the local data frame 530, thus in the multi-frame screen 500 of FIG. 8, the contents of the local data frame 530 would be the aforementioned first data group, which is the same as the scenario shown in FIG. 5.

[0127] In other words, in the multi-frame screen 500 shown in FIG. 8, the candidate object being currently selected in the navigator frame 510 is the candidate object 513, the first target global property data being currently displayed in the first global data frame 520 is the second device activity relationship diagram corresponding to the second date denoted by the candidate object 513, and the target data group being currently displayed in the local data frame 530 is the first data group corresponding to the computing device 111. In this situation, if the user selects the first main visual object 521 in the first global data frame 520 through the input device 145, the contents of the local data frame 530 would not change because the contents being currently displayed in the local data frame 530 are already the first data group corresponding to the computing device 111. However, if the user selects the second main visual object 523 in the first global data frame 520 through the input device 145, the frame association control module 350 would perform the operation 716 to instruct the local data frame generating module 340 to replace the local property data being currently displayed in the local data frame 530.

[0128] Then, the local data frame generating module 340 performs the operation 718 according to instructions of the frame association control module 350 to select a second data group corresponding to the computing device 112 denoted by the newly selected main visual object 523 to be the target data group, and to replace the contents of the local data frame 530 with the second data group corresponding to the computing device 112. The frame association control module 350 performs the operation 708 to control the display device 141 to display the updated contents of the local data frame 530, so that the contents of the multi-frame screen 500

are changed to be the scheme as shown in FIG. 9.

[0129] As the aforementioned, the frame association control module 350 would not request the navigator frame generating module 320 to consequentially change the contents of the multiple candidate objects in the navigator frame 510 in association with a change in the selected main visual object in the first global data frame 520. Thus, in the multi-frame screen 500 of FIG. 9, the contents of the navigator frame 510 would be the same as the contents in the scenario of FIG. 8 and thus remain unchanged.

[0130] In practice, the multi-frame screen 500 generated by the associated data frame generating program 154 may comprise multiple global data frames, and/or multiple local data frames at the same time. In the embodiment of FIG. 10, for example, the associated data frames generated by the associated data frame generating program 154 further comprise a second global data frame 1020 in addition to the aforementioned navigator frame 510, the first global data frame 520, and the local data frame 530.

[0131] As described previously, the global data frame generating module 330 may generate global property data of two or more than two types with respect to each filtering condition. For example, the global data frame generating module 330 may generate global property data of two different types with respect to each date.

[0132] When the currently selected candidate object in the navigator frame 510 is the candidate object 511, the global data frame generating module 330 may select the global property data of a first type corresponding to the first date denoted by the candidate object 511 to be the aforementioned first target global property data, and may further select the global property data of a second type corresponding to the first date to be a second target global property data. As shown in FIG. 10, the global data frame generating module 330 not only establishes the first global data frame 520 comprising the first target global property data, but also establishes a second global data frame 1020 comprising the second target global property data. In addition, when the frame association control module 350 controls the display device 141 to display the first global data frame 520, the frame association control module 350 also controls the display device 141 to display the second global data frame 1020 in the multi-frame screen 500 at the same time.

[0133] Similar to the scenario of the first global data frame 520, the global data frame generating module 330 utilizes the multiple main visual objects to respectively represent a portion of or all devices in the target network system 102 in the aforementioned second target global property data. The main visual objects generated by the global data frame generating module 330 in the second target global property data may have the same visual representation

with the main visual objects generated by the global data frame generating module 330 in the first target global property data, or may have different visual representations from the main visual objects in the first target global property data.

[0134] In other words, in the multi-frame screen 500 shown in FIG. 10, the candidate object being currently selected in the navigator frame 510 is the candidate object 511, the first target global property data being currently displayed in the first global data frame 520 is the global property data of the first type corresponding to the first date, and the second target global property data being currently displayed in the second global data frame 1020 is the global property data of the second type corresponding to the first date. In this situation, if the user selects the candidate object 513 in the navigator frame 510 through the input device 145, then the frame association control module 350 performs the operation 714 to instruct the global data frame generating module 330 to replace the first target global property data in the first global data frame 520 and the second target global property data in the second global data frame 1020.

[0135] Then, the global data frame generating module 330 performs the operation 614 according to the instruction of the frame association control module 350 to select the global property data of the first type corresponding to the second date denoted by the newly selected candidate object 513 to be the first target global property data, and to select the global property data of the second type corresponding to the second date to be the second target global property data. In addition, the global data frame generating module 330 further replaces the contents of the first global data frame 520 with the global property data of the first type corresponding to the aforementioned second date, and replaces the contents of the second global data frame 1020 with the global property data of the second type corresponding to the aforementioned second date. The frame association control module 350 performs the operation 708 to control the display device 141 to display the updated contents of both the first global data frame 520 and the second global data frame 1020, so that the contents of the multi-frame screen 500 are changed to be the scheme as shown in FIG. 11.

[0136] In the embodiment of FIG. 11, the frame association control module 350 would not instruct the local data frame generating module 340 to replace the target data group in the local data frame 530 in this situation, and thus the contents of the local data frame 530 shown in the multi-frame screen 500 of FIG. 11 are the same as the scenarios shown in FIG. 10.

[0137] In the aforementioned embodiments, the examples of the filtering conditions corresponding to the multiple candidate objects in the navigator frame 510 and the target data group in the local data frame 530 are merely an exemplary embodiment, rather than a restriction to the practical implementations. For example, FIG. 12 shows a simplified schematic diagram

of partial contents in the multiple-frame screens 500 according to another embodiment of the present disclosure. In the embodiment of FIG. 12, each of the filtering conditions corresponding to multiple exemplary candidate objects 1211~1215 in the navigator frame 510 is a device group which is classified based on a predetermined condition, while the target data group in the local data frame 530 are general information of the software and the hardware in a specific computing device.

[0138] In practice, the scheme of the filtering conditions corresponding to the multiple candidate objects in the navigator frame 510 as well as the scheme of the target data group in the local data frame 530 may be modified according to the requirement of the practical applications.

[0139] As can be appreciated from the foregoing descriptions, once the selected candidate object in the navigator frame 510 is changed, the contents of the first global data frame 520 would consequentially change in association with the change in the selected candidate object. Yet in this situation, the contents of the local data frame 530 may or may not consequentially change in association with the change in the selected candidate object, which is determined by the rule setting of the frame association control module 350.

[0140] On the other hand, once the selected main visual object in the first global data frame 520 is changed, the contents of the local data frame 530 would consequentially change in association with the change in the selected main visual object, but the contents of the navigator frame 510 would not change correspondingly.

[0141] Therefore, the cyber security analyst may adjust the combination of filtering conditions to be employed by changing the selected candidate objects in the navigator frame 510, and/or the selected main visual objects in the first global data frame 520, and observe the change in the contents of the data frames from the multi-frame screen 500 before and after adjusting the combination of filtering conditions.

[0142] From another aspect, when the selected candidate object in the navigator frame 510 is changed, it would cause an unidirectional change in the contents of the first global data frame 520, but when the selected main visual object in the first global data frame 520 is changed, it would not cause change in the contents of the navigator frame 510. The primary purpose of the aforementioned design with respect to the data frame association is to render that when the selected main visual object in the first global data frame 520 is changed to consequentially change the contents of the local data frame 530, the multiple candidate objects in the navigator frame 510 can be represented in the multi-frame screen 500 at the same time while not changing the contents of the candidate objects.

[0143] Such design is beneficial. The conventional analysis tools utilized by the cyber security analysts often require the cyber security analysts to conduct data filtering by inputting searching keywords. When the cyber security analysts change the filtering conditions, the former filtering conditions would be eliminated. Accordingly, the cyber security analysts need to memorize or keep records of the filtering conditions that have been used before, and it is difficult for the cyber security analysts to utilize a combination of hierarchical filtering conditions to conduct data filtering. Thus, in situations where there is a vast amount of data needed to be analyzed, the cyber security analysts need to repeatedly input same filtering conditions for many times, which apparently wastes considerable labor and time.

[0144] In comparison with the conventional approach, the multiple associated data frames 510~530 generated by the aforementioned associated data frame generating program 154 may represent the filtering conditions of different hierarchical levels in the multi-frame screen 500 at the same time. Therefore, it not only enables the cyber security analysts to be able to rapidly adjust a combination of the filtering conditions employed by manipulating the objects shown in the navigator frame 510 and the first global data frame 520, but also represents the filtering conditions of some hierarchical levels in the multi-frame screen 500 at the same time, so that the cyber security analysts can assess whether to change the filtering conditions at any time. Accordingly, the aforementioned data frame association approach is beneficial in reducing the time required for filtering a vast amount of data, it is particularly beneficial in increasing the overall determining efficiency in diagnosing whether or not a specific network environment is breached by hackers.

[0145] In addition, the associated data frame generating program 154 conducts analysis on the multiple suspicious activities records related to the target network system 102, the corresponding multiple time stamps, and the corresponding multiple attribute tags, filters out unnecessary noisy data, and further generates the navigator frame 510 for displaying multiple filtering conditions, the first global data frame 520 for displaying specific global property data related to a portion of or all devices in the target network system 102, and the local data frame 530 for displaying a specific data group corresponding to one of the computing devices in the target network system 102. In this way, the multiple associated data frames 510~530 generated by the aforementioned associated data frame generating program 154 can significantly reduce the data volume that the cyber security analysts need to pay attention to, and therefore can effectively mitigate the problem that numerous noisy data interferes the cyber security analysts.

[0146] Additionally, since the associated data frame generating program 154 controls the display device 141 to display the aforementioned navigator frame 510, the first global data

frame 520, and the local data frame 530 at the same time, the cyber security analysts can acquire important reference data related to the target network system 102 from different aspects or different dimensions at the same time from the contents of the navigator frame 510, the first global data frame 520, and the local data frame 530, which is beneficial in improving the efficiency in the diagnosing process.

[0147] Furthermore, according to the research in the cognitive science, human beings have higher efficiency in understanding visualized information than understanding information presented in the form of pure texts. Since the multiple associated data frames 510~530 generated by the associated data frame generating program 154 can represent the aforementioned reference information of multiple dimensions in a straightforward visualized manner to the cyber security analysts, it is beneficial in significantly reducing the time required by the cyber security analysts in analyzing the digital evidences, thereby effectively improving the efficiency in diagnosing whether the target network system 102 is breached by hackers.

[0148] Please note that the execution order of the operations in the aforementioned FIG. 6 and FIG. 7 is merely an exemplary embodiment, rather than a restriction to the practical implementations. For example, in FIG. 6, the execution order of the operations 602 and 604 has no particular association with the execution order of the operations 606 through 612, thus the operations 606 through 612 may be performed prior to the operations 602 and 604. For another example, the execution order of the operations 602 and 604 has no particular association with the execution order of the operations 702 through 706, thus the operations 702 through 706 may be performed prior to the operations 602 and 604. For yet another example, the execution order of the operations 606 through 612 has no particular association with the execution order of the operations 702 through 706, thus the operations 702 through 706 may be performed prior to the operations 606 through 612. For yet another example, the execution order of the operations 610 and 612 may be swapped, or alternatively, the operations 610 and 612 may be performed at the same time. For yet another example, in FIG. 7, the execution order of the operations 710 and 712 may be performed in turns, or alternatively, the operations 710 and 712 may be performed at the same time.

[0149] In the aforementioned embodiments, the multiple attribute tags corresponding to the multiple suspicious activities records are set by the device activities reporting program 120 installed in the respective computing devices in the operation 404, but this is merely an exemplary embodiment, rather than a restriction to the practical implementations.

[0150] In practice, the operation 404 may alternatively be performed by the activity records collection device 130. That is, in the operations of the aforementioned FIG. 4, the device

activities reporting program 120 only needs to perform the operations 402 and 406, while the device activities reporting program 120 only needs to transmit the suspicious activities records and the corresponding time stamps to the activity records collection device 130 in the operation 406. After the activity records collection device 130 receives the suspicious activities records and the corresponding time stamps, the activity records collection device 130 may perform the operation 404 to create multiple attribute tags respectively corresponding to the multiple suspicious activities records.

[0151] In some embodiments, the data stored in the database 152 may be loaded into the database 152 through other approaches, and not limited to be received by the communication circuit 143 of the aforementioned multi-frame cyber security analysis device 140. In this situation, the communication circuit 143 may be omitted.

[0152] In some application environments where the quantity of the computing devices in the target network system 102 is small, or the target network system 102 has sufficient networking bandwidth with external networks, the activity records collection device 130 in the cyber breach diagnostics system 100 may be omitted.

[0153] For example, FIG. 13 shows a simplified functional block diagram of the cyber breach diagnostics system 100 according to another embodiment of the present disclosure. In the embodiment of FIG. 13, the activity records collection device 130 in the aforementioned FIG. 1 is omitted, and the operations 408~412, which are previously performed by the activity records collection device 130, can be instead performed by respective device activities reporting programs 120. In other words, in the cyber breach diagnostics system 100 in FIG. 13, the device activities reporting program 120 installed in the respective computing devices processes the multiple suspicious activities records, the multiple time stamps, and the multiple attribute tags so as to generate the return data, and to transmit the return data to the multi-frame cyber security analysis device 140 through appropriate networks (e.g., the internet).

[0154] The foregoing descriptions regarding the connections, implementations, operations, and related advantages of other components in FIG. 1 are also applicable to the embodiment in FIG. 13. For the sake of brevity, those descriptions will not be repeated here.

[0155] Certain terms are used throughout the description and the claims to refer to particular components. One skilled in the art appreciates that a component may be referred to as different names. This disclosure does not intend to distinguish between components that differ in name but not in function. In the description and in the claims, the term “comprise” is used in an open-ended fashion, and thus should be interpreted to mean “include, but not limited to.” The term “couple” is intended to compass any indirect or direct connection. Accordingly, if this

disclosure mentioned that a first device is coupled with a second device, it means that the first device may be directly or indirectly connected to the second device through electrical connections, wireless communications, optical communications, or other signal connections with/without other intermediate devices or connection means.

[0156] The term “and/or” may comprise any and all combinations of one or more of the associated listed items. In addition, the singular forms “a,” “an,” and “the” herein are intended to comprise the plural forms as well, unless the context clearly indicates otherwise.

[0157] Other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the invention indicated by the following claims.

CLAIMS

What is claimed is:

1. A multi-frame cyber security analysis device (140) for diagnosing whether a target network system (102) is breached by hackers, the multi-frame cyber security analysis device (140) comprising:

a display device (141);

an input device (145), arranged to operably receive operation commands issued by a user;

a non-volatile storage circuit (147), arranged to operably store a database (152) and an associated data frame generating program (154), wherein the database (152) is stored with device activities records of multiple types related to multiple computing devices (111~115) in the target network system (102); and

a control circuit (149), coupled with the display device (141), the input device (145), and the non-volatile storage circuit (147), and arranged to operably execute the associated data frame generating program (154), so as to conduct data frame generating operation according to the device activities records of multiple types stored in the database (152) to generate multiple associated data frames (510, 520, 530, 1020) related to the target network system (102) and to display contents of the multiple associated data frames (510, 520, 530, 1020) at the same time;

wherein the multiple associated data frames (510, 520, 530, 1020) comprise a navigator frame (510), a first global data frame (520), and a local data frame (530).

2. The multi-frame cyber security analysis device (140) of claim 1, wherein the data frame generating operation comprises:

generating multiple candidate objects (511, 513, 515) respectively corresponding to multiple filtering conditions, wherein the multiple candidate objects (511, 513, 515) comprise a first candidate object (511) corresponding to a first filtering condition, and a second candidate object (513) corresponding to a second filtering condition;

establishing a navigator frame (510) comprising the multiple candidate objects (511, 513, 515);

generating multiple global property data related to a portion of or all devices in the target network system (102) according to data stored in the database (152), wherein the multiple global property data comprise a first global property data corresponding to the

first filtering condition, and a second global property data corresponding to the second filtering condition;

selecting one of the multiple global property data as a first target global property data;

establishing a first global data frame (520) comprising the first target global property data;

in the first target global property data, respectively utilizing multiple main visual objects (521, 523, 525) to represent a portion of or all devices in the target network system (102), wherein the main visual objects comprise a first main visual object (521) corresponding to a first computing device (111), and a second main visual object (523) corresponding to a second computing device (112);

generating multiple data groups respectively corresponding to the multiple computing devices (111~115) according to data stored in the database (152), wherein the multiple data groups comprise a first data group corresponding to the first computing device (111), and a second data group corresponding to the second computing device (112);

selecting one of the multiple data groups as a target data group;

establishing a local data frame (530) comprising the target data group;

utilizing the display device (141) to display contents of the navigator frame (510), the first global data frame (520), and the local data frame (530) at the same time; and

controlling an associated relationship among the navigator frame (510), the first global data frame (520), and the local data frame (530) to render contents of the first global data frame (520) to change when the navigator frame (510) is manipulated by the user, contents of the local data frame (530) to change when the first global data frame (520) is manipulated by the user, but contents of the navigator frame (510) not to change when the first global data frame (520) is manipulated by the user.

3. The multi-frame cyber security analysis device (140) of claim 2, wherein the data frame generating operation further comprises:

in a situation of that a candidate object being currently selected in the navigator frame (510) is the first candidate object (511) and the first target global property data being currently displayed in the first global data frame (520) is the first global property data, if the user then selects the second candidate object (513) in the navigator frame (510) through the input device (145), replacing the first target global property data being currently displayed in the first global data frame (520) with the second global property data corresponding to the second filtering condition .

4. The multi-frame cyber security analysis device (140) of claim 3, wherein the data frame generating operation further comprises:

in a situation of that the first target global property data being currently displayed in the first global data frame (520) is the second global property data, a main visual object being currently selected in the first global data frame (520) is the first main visual object (521), and the target data group being currently displayed in the local data frame (530) is the first data group, if the user then selects the second main visual object (523) in the first global data frame (520) through the input device (145), replacing the target data group being currently displayed in the local data frame (530) with the second data group corresponding to the second computing device (112), but not changing contents of the navigator frame (510).

5. The multi-frame cyber security analysis device (140) of claim 3, wherein the data frame generating operation further comprises:

replacing the target data group being currently displayed in the local data frame (530) with a predetermined data group corresponding to the second filtering condition.

6. The multi-frame cyber security analysis device (140) of claim 3, wherein the multiple global property data further comprise a third global property data corresponding to the first filtering condition and a fourth global property data corresponding to the second filtering condition, and the data frame generating operation further comprises:

selecting the third global property data as a second target global property data;

establishing a second global data frame (1020) comprising the second target global property data;

displaying the second global data frame (1020) at the same time when displaying the first global data frame (520); and

in the second target global property data, respectively utilizing multiple main visual objects (521, 523, 525) to represent a portion of or all devices in the target network system (102).

7. The multi-frame cyber security analysis device (140) of claim 6, wherein the data frame generating operation further comprises:

in a situation of that a candidate object being currently selected in the navigator frame (510) is the first candidate object (511), the first target global property data being currently displayed in the first global data frame (520) is the first global property data, and the

second target global property data being currently displayed in the second global data frame (1020) is the third global property data, if the user then selects the second candidate object (513) in the navigator frame (510) through the input device (145), replacing the first target global property data being currently displayed in the first global data frame (520) with the second global property data corresponding to the second filtering condition and also replacing the second target global property data being currently displayed in the second global data frame (1020) with the fourth global property data corresponding to the second filtering condition.

8. A non-transitory computer program product (154), stored in a non-volatile storage circuit (147) of a multi-frame cyber security analysis device (140) and enabling the multi-frame cyber security analysis device (140) to conduct a data frame generating operation according to device activities records of multiple types stored in a database (152), so as to generate multiple associated data frames (510, 520, 530, 1020) related to a target network system (102), and to display contents of the multiple associated data frames (510, 520, 530, 1020) at the same time, wherein the multiple associated data frames (510, 520, 530, 1020) comprise a navigator frame (510), a first global data frame (520), and a local data frame (530).

9. The computer program product (154) of claim 8, wherein the data frame generating operation comprises:

generating multiple candidate objects (511, 513, 515) respectively corresponding to multiple filtering conditions, wherein the multiple candidate objects (511, 513, 515) comprise a first candidate object (511) corresponding to a first filtering condition, and a second candidate object (513) corresponding to a second filtering condition;

establishing a navigator frame (510) comprising the multiple candidate objects (511, 513, 515);

generating multiple global property data related to a portion of or all devices in the target network system (102) according to data stored in the database (152), wherein the multiple global property data comprise a first global property data corresponding to the first filtering condition, and a second global property data corresponding to the second filtering condition;

selecting one of the multiple global property data as a first target global property data;

establishing a first global data frame (520) comprising the first target global property data;

in the first target global property data, respectively utilizing multiple main visual objects (521, 523, 525) to represent a portion of or all devices in the target network system (102), wherein the main visual objects comprise a first main visual object (521) corresponding to a first computing device (111), and a second main visual object (523) corresponding to a second computing device (112);

generating multiple data groups respectively corresponding to the multiple computing devices (111~115) according to data stored in the database (152), wherein the multiple data groups comprise a first data group corresponding to the first computing device (111), and a second data group corresponding to the second computing device (112);

selecting one of the multiple data groups as a target data group;

establishing a local data frame (530) comprising the target data group;

utilizing the display device (141) to display contents of the navigator frame (510), the first global data frame (520), and the local data frame (530) at the same time; and

controlling an associated relationship among the navigator frame (510), the first global data frame (520), and the local data frame (530), to render contents of the first global data frame (520) to change when the navigator frame (510) is manipulated by the user, and contents of the local data frame (530) to change when the first global data frame (520) is manipulated by the user, but contents of the navigator frame (510) not to change when the first global data frame (520) is manipulated by the user.

10. The computer program product (154) of claim 9, wherein the data frame generating operation further comprises:

in a situation of that a candidate object being currently selected in the navigator frame (510) is the first candidate object (511) and the first target global property data being currently displayed in the first global data frame (520) is the first global property data, if the user then selects the second candidate object (513) in the navigator frame (510) through the input device (145), replacing the first target global property data being currently displayed in the first global data frame (520) with the second global property data corresponding to the second filtering condition.

11. The computer program product (154) of claim 10, wherein the data frame generating operation further comprises:

in a situation of that the first target global property data being currently displayed in the first global data frame (520) is the second global property data, a main visual object being

currently selected in the first global data frame (520) is the first main visual object (521), and the target data group being currently displayed in the local data frame (530) is the first data group, if the user then selects the second main visual object (523) in the first global data frame (520) through the input device (145), replacing the target data group being currently displayed in the local data frame (530) with the second data group corresponding to the second computing device (112), but not changing contents of the navigator frame (510).

12. The computer program product (154) of claim 10, wherein the data frame generating operation further comprises:

replacing the target data group being currently displayed in the local data frame (530) with a predetermined data group corresponding to the second filtering condition.

13. The computer program product (154) of claim 10, wherein the multiple global property data further comprise a third global property data corresponding to the first filtering condition and a fourth global property data corresponding to the second filtering condition, and the data frame generating operation further comprises:

selecting the third global property data as a second target global property data;

establishing a second global data frame (1020) comprising the second target global property data;

displaying the second global data frame (1020) at the same time when displaying the first global data frame (520); and

in the second target global property data, respectively utilizing multiple main visual objects (521, 523, 525) to represent a portion of or all devices in the target network system (102).

14. The computer program product (154) of claim 13, wherein the data frame generating operation further comprises:

in a situation of that a candidate object being currently selected in the navigator frame (510) is the first candidate object (511), the first target global property data being currently displayed in the first global data frame (520) is the first global property data, and the second target global property data being currently displayed in the second global data frame (1020) is the third global property data, if the user then selects the second candidate object (513) in the navigator frame (510) through the input device (145), replacing the first target global property data being currently displayed in the first global data frame

(520) with the second global property data corresponding to the second filtering condition and also replacing the second target global property data being currently displayed in the second global data frame (1020) with the fourth global property data corresponding to the second filtering condition.