

- [0131] 3. In step 432, the procedure compares the obtained address with the previously recorded procedure-address of the same object in knowledge base 150.
- [0132] 4. If a match of the procedure-address is found in step 432, no alert is issued, and the operation returns to step 430, to check the next relevant occurrence of this type.
- [0133] 5. If no match is found in step 432 due to non-existence of procedure-address of the same object within knowledge base 150, and if there are no other signs in knowledge base 150 of a suspected breach, it is assumed that this is not a sign for a breach, and the obtained procedure-address is recorded within knowledge base 150 for a future use. In some other cases, however, this may be considered as a suspected sign, and the user is notified accordingly.
- [0134] 6. If the enumeration comparison of step 432 shows that the enumeration does not match, the procedure continues to step 434.
- [0135] 7. In step 434, the name of the SCR that contains the new procedure-address is obtained. If, however, the name of the SCR cannot be obtained for some reason, an alert is issued (in step 437).
- [0136] 8. In step 435, the SCR which has been found to be containing the new procedure-address is evaluated. The evaluation may include several tests, such as, the SCR function, its structure, etc. The evaluation of this stage may use data stored in knowledge base 150, in order to characterize that SCR. That SCR is at relatively high odds of being an added SCR that was not caught at the moment of addition. If the evaluation shows that the SCR is suspected, an alert is issued in step 437. Otherwise, the procedure continues to step 436, which does not issue an alert, and continues in supervising the shared code activity in step 430.
- [0137] In the Embodiment of FIG. 4D
- [0138] This embodiment of the invention discloses a public sensor for passive direct approach offender with first setting and/or with second setting, according to the preferred embodiment of the invention:
- [0139] Typically, when an SCR, such as the SCR that is being suspected as an offender, is engaged in either processor-intensive or IO-intensive activity and is not using a separate thread, the performance of the process is due to degrade. The public sensor looks for statistical evidence of both degradation in expected normal performance and increased abnormal activities of processes while they are executing.
- [0140] The procedure of the embodiment of FIG. 4D shows the detection and evaluation of degrading performance or exceeding resource-consumption within a given task. The procedure checks the activity of the counters dealing with the stack operation. For example, the activity of the counters during the activation of a stack is characterized, and compared with statistical information previously accumulated and recorded in knowledge base 150 regarding the operation of same stack. If a deviation beyond a predefined threshold is found, an alert is issued.
- [0141] 1. In step 440, the sensor checks whether enough parameters are available for carrying out the test.
- [0142] 2. In step 441, the activity of the counters dealing with the activation of either the monitored SCR-chains or the specifically monitored processes is characterized. Some parameters that are checked are: their speed of operation, the manner of their incrementing, the load on the system's memory, on the processor(s), the disk activity, etc.
- [0143] 3. In step 442, the procedure compares the obtained characteristics with corresponding statistical characteristics previously accumulated, using a standard deviation. If a deviation above a predefined threshold value is found, the procedure continues to step 447. If, however, no record is found for comparison, the obtained information is recorded (step 443) in knowledge base 150, and the procedure continues to step 446, in which no alert is issued. If in step 442 the information is found to be within the predefined statistical threshold range, knowledge base 150 is statistically updated by the new data, and the procedure continues to step 446, in which no alert is issued. From step 446 the procedure returns to step 440, and the procedure initiates the test again for any new occurrence of the same type.
- [0144] In the Embodiment of FIG. 4E
- [0145] A suspect SCR may launch new threads to conceal its activity, because multithreading enables relatively smooth operation when compared to the sequential execution of extra code. The sensor looks for suspicious signs, like a new thread being created under a process context.
- [0146] The procedure of FIG. 4E illustrates the detection and evaluation of a new thread created in the context of a given process. In some cases, when this is not a normal activity of the process, it may indicate an offender SCR trying to hide its extra activity by performing it on a separate thread. During the following activation of a process, the procedure of FIG. 4E compares the current threads with the threads as recorded, and alerts if it finds new ones. Getting the name of the SCR that stores the instructions that are run directly by the new thread, or the SCR that has issued the instruction of creating the new thread is not guaranteed: failing to get that name leads directly to an alert.
- [0147] 1. In step 450, the sensor checks whether enough parameters are available for carrying out the test.
- [0148] 2. In step 451, the sensor enumerates the threads as created by the present process.
- [0149] 3. In step 452, the procedure compares the obtained thread enumeration with the corresponding thread enumeration previously recorded in knowledge base 150 for that process. If a match is found, the procedure continues to step 457, in which no alert is issued. If no thread enumeration record is found for that specific process, the found thread enumeration is recorded (step 453). If, however, no matching is found, the procedure continues to step 454.
- [0150] 4. In step 454, the procedure tries to obtain the name of the SCR that stores the instructions that are run directly by the new thread, or the SCR that has issued the instruction of creating the new thread. If the procedure fails to get the new SCR name, an alert is issued