

- [0110] 1. In step 410, the sensor checks whether enough parameters are available for carrying out the test.
- [0111] 2. In step 411, the procedure enumerates the SCRs mapped into the currently running process, giving both the total number of SCRs and, preferably, also their order. If the enumeration is successfully obtained, the procedure continues to step 412.
- [0112] 3. In step 412, the procedure compares the obtained enumeration with the previously recorded SCR enumeration of same SCR list in knowledge base 150.
- [0113] 4. If a match of the enumeration is found in step 412, the procedure assumes that the stack operation is legal, no alert is issued, and the operation returns to step 410, to check the next available occurrence of this type.
- [0114] 5. If no match is found in step 412 due to non-existence of SCR enumeration record of said stack 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 enumeration 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.
- [0115] 6. If the enumeration verification of step 412 shows no enumeration match, the procedure continues to step 414.
- [0116] 7. In step 414, the name of the SCR that has been found to be added to the stack is obtained. If, however, the name of the new SCR cannot be obtained for some reason, an alert is issued (in step 417).
- [0117] 8. In step 415, the SCR which has been found to be added to the process 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 the added SCR. Of course, if more than one SCR is found to be added, the procedure is carried out separately for each SCR. If the evaluation shows that the SCR is suspected, an alert is issued in step 417. Otherwise, the procedure continues to step 416, which does not issue an alert, and continues in supervising the shared code activity in step 410.
- [0118] In the Embodiment of FIG. 4B:
- [0119] In some cases, the Operating System enables an on-line identification of the occurrence of adding an SCR to a functional-stack chain during operation. The embodiment of FIG. 4B, is applicable for the case when the operating system enables obtaining a detailed list of SCRs in a given functional chain. The procedure therefore checks the available list, and if new, suspected SCRs are found within the list, an alert is issued. Initial checking of SCR chains by this embodiment, unlike initial checking of processes by the embodiment of FIG. 4A, should be done when the system is booting, and assumed to be free of breaches.
- [0120] 1. In step 420, the sensor checks whether enough parameters are available for carrying out the test.
- [0121] 2. In step 421, the procedure enumerates the SCRs within a specific chain, giving both the total number of SCRs and, preferably, also their order. If the enumeration is successfully obtained, the procedure continues to step 422.
- [0122] 3. In step 422, the procedure compares the obtained enumeration with the previously recorded SCR enumeration of same chain in knowledge base 150.
- [0123] 4. If a match of the enumeration is found in step 422, the procedure assumes that the addition of the SCR to the chain is legal, no alert is issued, and the operation returns to step 420, to check the next relevant occurrence of this type.
- [0124] 5. If the enumeration comparison of step 422 shows that the enumeration does not match, the procedure continues to step 424.
- [0125] 6. In step 424, the name of the SCR that has been found to be added to the chain is obtained. If, however, the name of the new SCR cannot be obtained for some reason, an alert is issued (in step 427).
- [0126] 7. In step 425, the SCR which has been found to be added to the chain 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 the added SCR. Of course, if more than one SCR is found to be added, the procedure is carried out separately for each SCR. If the evaluation shows that the SCR is suspected, an alert is issued in step 427. Otherwise, the procedure continues to step 426, which does not issue an alert, and continues in supervising the shared code activity in step 420.
- [0127] In the Embodiment of FIG. 4C
- [0128] In some cases, the Operating System enables a change in the logic of a process by replacing the address of the procedure of one of its user mode components (e.g., a parent window, or one of its children). More particularly, one of the tasks of a modern Operating System is to manage multiple user-tasks through multiple windows. The following refers essentially to Windows™. The "user" part of the Operating System routes messages to and from different windows. Each window has its message loop waiting for incoming messages. Of course when the address pointing to the procedure that implements that loop in a given window is altered, the whole behavior or function of the window is altered without providing a proper notification to the user. This is one of the typical hostile activities that a sophisticated offender may wish to exercise after breaching the memory address space of a process by inserting a hostile SCR in one of the stacks connected to that process. The embodiment of FIG. 4C does not assume that the system may provide a notification on such a symptom, and it also assumes that the breach has already occurred, either without being notified or it was notified but at the time of the breach there was not enough evidence to cause an alert.
- [0129] 1. In step 430, the sensor checks whether enough parameters are available for carrying out the test.
- [0130] 2. In step 431, the procedure tries to obtain the current procedure-address for a given object. If the address is successfully obtained, the procedure continues to step 432.