

operation of the stack, or breaking the connection between the active chain and the application 52.

[0079] As shown, whenever the suspect SCR is successfully implanted within the chain by an offender, it, for example, is capable of transferring information to another process of the offender via connection 178. However, the private sensor 41 and the public sensor 25 are capable, according to the invention, of breaking the connection between the suspect SCR 27 and the suspect process 51. The public sensor 25 is a sensor common to a plurality of stacks and it can receive information from the SCR probe 26 in similarity to the private sensor 41. It should be noted that it is important for the SCR probe 26 to be installed as close as possible, whenever the OS enables it, to the beginning of the chain, indicated by SCR 21.

[0080] The private sensor 41 is implemented as a common component, which may be coupled with call stack 1 in the kernel-mode. More particularly, the private sensor 41 is actually a hybrid: coupling the top-level input-element with a low-level kernel-mode module (or a user-mode 'base provider' when it is guaranteed to stay lowest), using encryption/decryption to (I) detect unauthorized manipulators and (II) to provide more 'passive' security against silent eavesdroppers. Providing 'trusted' SCRs with a private/public key pair can help indicating when an infiltrator has messed with I/O, especially if those keys are 'short lived': valid for only a limited short period of time.

[0081] Note: In all the following flow diagrams, when a loop arrow such as "no signal" arrow of block 221 of FIG. 2c appears, it indicates that the procedures stays in the same block until the block receives a new input or condition, in which it again performs its related operation.

[0082] FIG. 2C illustrates the interaction between the probe 26 and the sensor main unit 25. Initially, in step 221 the sensor main unit 25 creates the probe, which is essentially an SCR, and implants it within the stack. The sensor main unit 25 then waits for a call from probe 26. It should be noted that the main unit 25 may create and control a plurality of probes, one for each stack, or a plurality of main units 25, each having one probe 26, may be formed. At this stage, when the stack is activated, the probe begins in step 222 to evaluate changes in the activated stack, and looks for the existence of a possible suspect SCR. If an abnormal condition is found in step 222, in step 223 the probe freezes the activity of the stack, including all its SCR components. In the next step, 224, the probe 26 flushes or transfers the records collected by the probe either to the main unit 25 or to a local storage maintained by the probe 26 itself. In step 225, the probe 26 calls the main unit 25. In block 333, the main unit 25 transfers the received records to the decision unit 29, for evaluation. In step 226, the probe 26 waits for a conclusion made by the decision unit 29. When such a conclusion is available, it is conveyed in step 334 to probe 26. If the conclusion shows that the stack activity is valid, the main unit 25 releases the previously frozen activity in step 227, otherwise an alert is initiated in step 227, or the stack is further supervised as suspected.

[0083] FIG. 3 illustrates in a flow diagram form the evaluation of a signal by probe 26, according to an embodiment of the invention. As previously noted, a 'signal' in this context is an indication given by the OS about some particular state transition. Initially (not shown), a range of

operation for the checking by the probe is defined. The range relates to the parameters that are checked, their value, etc. and definition is made with respect to the conditions where a further check is needed. It should be noted that not all signals are handled by each sensor; rather, each sensor has a 'range' of signals which it can handle. This range is implemented generally by a simple table or list that is saved in knowledge base 150. Next, in block 31, probe 26 checks whether a condition has been detected that justifies a further checking. If not, the procedure stays in block 31 until the occurrence of an event indicating that the checked parameters are within the predefined checking range. If a condition within the range of checking has been detected, the procedure continues to block 32.

[0084] If a suspected SCR is detected, the procedure obtains in block 32 its name. Whenever the name of the suspected SCR is available, a verification is made in step 33 in a list of invalid SCRs of knowledge base 150 to find whether the found SCR is listed there. Searching the said list, leads to one of the following three options:

[0085] First option: The SCR is found in the list of suspected SCRs within the knowledge base 150. In that case, the procedure continues to block 29 for a further test.

[0086] Second option: The SCR is not found in the list of invalid SCRs or in the list of valid SCRs within the knowledge base 150. In that case the procedure also continues to block 29 for a further test.

[0087] Third option: the SCR is listed in the list of valid (authorized) SCRs. In that case, a signature test is performed in step 35. If the SCR pass the signature test, it is assigned as a valid SCR in block 37. If, however, the SCR does not pass the test, the procedure continues to step 29 for a further test.

[0088] In step 29 a further test is performed until a decision is obtained. In step 39, if the test of step 29 shows that the SCR is valid, the SCR is added in step 37 to the list of authorized SCRs in knowledge base 150. If however the test shows that the SCR is unauthorized, its name (and optionally other characteristics of it) is first added in step 38 to the list of unauthorized SCRs, and an alert is initiated in step 417.

[0089] FIG. 5 is a block diagram illustrating the general operation of the decision unit 29. In block 291, decision unit 29 monitors the probe 26. As long as there are no suspected symptoms, the operation of unit 29 stays in block 291. Generally, the monitoring of probe 26 can obtain one or more of the following symptoms:

[0090] Negative symptoms, i.e., unsuspected symptoms that indicate that there are no signs for offenders or offending activities.

[0091] Positive symptoms, i.e., assured symptom of suspected offender.

[0092] Fuzzy symptoms, i.e., non-decisive symptoms, which can not provide certain indication whether an offender or suspected symptoms exist.

[0093] It is important to note that upon detecting a fuzzy symptom or a positive symptom by probe 26, the sensor mechanism may freeze the action of the invader, the invaded