

which is described herein spreads concurrently upon different threads in different processes. An 'instance' of the DLL should therefore examine its own thread ID against thread IDs that come from other participants. Global storage for these IDs, as well as other inter-thread or inter-process variables, may be provided either by a shared section inside the DLL, or by some 'named' object such as a named memory mapped file.

[0201] The above examples and description have of course been provided only for the purpose of illustration, and are not intended to limit the invention in any way. As will be appreciated by the skilled person, the invention can be carried out in a great variety of ways, employing more than one technique from those described above, all without exceeding the scope of the invention.

1. A method for detecting and eliminating SCR breach operations by a second party within the memory space allocated to a first party, in a multi-tasking system, comprising:

- a. Pre-recording by said first party within a knowledge base the structure and/or behavior of an SCR stack;
- b. Implanting within the SCR stack a dedicated SCR for reporting on the structure and/or behavior of said SCR stack when said SCR stack is activated;
- c. When said SCR stack is activated, comparing the data reported by said dedicated SCR with the said pre-recorded stack structure and/or behavior; and
- d. Whenever non-matching in the structure and/or behavior is found step c, ceasing the activity of said activated stack, and alerting.

2. A method according to claim 1, wherein the comparison of structure comprises verification of one or more of the following:

- the number of SCRs within the stack;
- the chain order of the SCRs within the stack;
- the time-stamps of the SCRs within the stack;
- the names of the SCRs within the stack;
- a signature of each SCR within the stack;
- the number of bits of each SCR within the stack;
- a checksum of each SCR within the stack; and
- the physical path and name of each SCR within the stack.

3. A method according to claim 1, wherein the comparison of behavior comprises verification of one or more of the following:

- duration of performance of the stack, and/or each SCR within the stack; and
- the I/O devices and/or addresses to which a communication is made when the stack is activated by a specific process.

4. A method according to claim 1, wherein the SCR breach operation is carried out by means of implanting SCRs within a shared stack by said second party.

5. A method according to claim 1, wherein the SCR breach operation is carried out by means of implanting by said second party an SCR within a shared stack supposed to be activated by said first party, and wherein the SCR implanted by said second party is designed to perform operations within the memory space exclusively allocated to said first party.

6. A method according to claim 1, wherein the SCR breach operation is carried out by means of manipulating by said second party an SCR within a shared stack supposed to be activated by said first party, and wherein the SCR manipulated by said second party is designed to perform operations within the memory space exclusively allocated to said first party.

7. A method according to claim 1, which is performed with respect to each stack supposed to be activated by said first party.

8. A method according to claim 1, wherein the stack behavior is checked independent of the process activating it.

9. A method according to claim 1, wherein the stack behavior is checked specifically with respect to the process activating it.

10. A sensor for detecting and eliminating SCR breach operations by a second party within the memory space allocated to a first party, in a multi-tasking system, comprising:

- a. At least one probe implanted within a stack by said first party, for reporting on the structure and/or behavior of said SCR stack, when said SCR stack is activated;
- b. A knowledge base for containing information relating to the structure and/or behavior of the stack, when activated;
- c. A comparing unit for comparing information relating to the stack structure and/or behavior as reported by the probe, with information recorded in said database; and
- d. A decision unit capable of initiating one or more of the following operations, if abnormal structure and/or behavior of the active stack is detected in step c:

 Ceasing operation of the active stack;

 Alerting the user of the detection of an abnormal structure and/or behavior of the active stack;

 Analyzing the operation of the active stack to detect the second party that originated the SCR breach operation; and

 Informing other fellow agents.

11. A system comprising a plurality of sensors according to claim 10.

12. A sensor according to claim 10, comprising a plurality of probes implanted each within one stack.

* * * * *