

ABSTRACT

A method for preventing malicious software from execution within a computer system is disclosed. A permutation is performed on a subset of instructions within an application program to yield a permuted sequence of instructions before any actual execution of the application program on the computer system. A permutation sequence number of the permuted sequence of instructions is stored in a permuted instruction pointer table. The permuted sequence of instructions is executed in an execution module that is capable of translating the permuted sequence of instructions to an actual machine code of a processor within the computer system according to the permutation sequence number of the permuted sequence of instructions stored in the permuted instruction pointer table.

A method for preventing malicious software from execution within a computer system is disclosed. Before any actual execution of an application program on a computer system, the application program needs to be cross-compiled to yield a set of cross-compiled code of the application program. The set of cross-compiled code of the application program can then be executed in an execution module that is capable of recognizing and translating the set of cross-compiled code of the application program to the actual machine code of the processor.



162162



G00002