

CLAIMS

1. A host system comprising at least one hardware processor configured to execute a virtual machine and a computer security program, wherein the at least one hardware processor is further configured to:

in response to receiving a guest instruction for execution, determine whether executing the guest instruction within the virtual machine causes a violation of a memory access permission, the guest instruction instructing the at least one hardware processor to determine a result of applying an operator to an operand, wherein executing the guest instruction in the absence of the violation causes writing the result to a first location;

in response to determining whether executing the guest instruction causes the violation, when executing the guest instruction causes the violation, write the result to a second location distinct from the first location, the second location accessible to the computer security program; and

in response to writing the result to the second location, switch from executing the guest instruction to executing the computer security program, wherein the computer security program is configured to determine whether the violation is indicative of a computer security threat.
2. The host system of claim 1, wherein the first location is a general purpose register of the at least one hardware processor.
3. The host system of claim 1, wherein the first location is a control register of the at least one hardware processor.
4. The host system of claim 1, wherein the first location comprises a section of a memory of the host system.
5. The host system of claim 1, wherein the result comprises a memory address.
6. The host system of claim 1, wherein the result comprises the operand.

7. The host system of claim 1, wherein the computer security program executes within the virtual machine.
8. The host system of claim 1, wherein the computer security program executes outside the virtual machine.
9. The host system of claim 1, wherein the second location comprises a predetermined register of the at least one hardware processor.
10. The host system of claim 1, wherein the second location comprises a predetermined section of a memory of the host system.
11. The host system of claim 1, wherein the second location comprises a data structure indicative of a current state of the virtual machine.
12. The host system of claim 1, wherein the at least one hardware processor is further configured, in response to switching to executing the computer security program, to read the result from the second location.
13. The host system of claim 12, wherein the at least one hardware processor is further configured, in response reading the result, to write the result to a destination determined according to the guest instruction.
14. The host system of claim 1, wherein the computer security program comprises an instruction which, when executed by the at least one hardware processor, causes the at least one hardware processor to read the result from the second location and to write the result to a destination determined according to the guest instruction.
15. The host system of claim 1, wherein the at least one hardware processor is further configured, in response to switching to executing the computer security program, to:

determine whether the guest instruction is an atomic instruction; and

in response, when the guest instruction is an atomic instruction, to execute the guest instruction within the virtual machine.
16. A method of protecting a host system from computer security threats, the method comprising:

in response to receiving a guest instruction for execution, employing at least one hardware processor of the host system to determine whether executing the guest instruction causes a violation of a memory access permission, wherein the guest instruction executes within a guest virtual machine exposed by the host system, the guest instruction instructing the at least one hardware processor to determine a result of applying an operator to an operand, wherein executing the guest instruction in the absence of the violation causes writing the result to a first location;

in response to determining whether executing the guest instruction causes the violation, when executing the guest instruction causes the violation, employing the at least one hardware processor to write the result to a second location distinct from the first location, the second location accessible to the computer security program; and

in response to writing the result to the second location, switching from executing the guest instruction to executing the computer security program, wherein the computer security program is configured to determine whether the violation is indicative of a computer security threat.

17. The method of claim 16, further comprising, in response to switching to executing the computer security program, employing the at least one hardware processor to read the result from the second location.
18. The method of claim 17, further comprising, in response to reading the result, employing the at least one hardware processor to write the result to a destination determined according to the guest instruction.
19. At least one hardware processor of a host system, the at least one hardware processor configurable to:

in response to receiving a guest instruction for execution, determine whether executing the guest instruction causes a violation of a memory access permission, wherein the guest instruction executes within a guest virtual machine exposed by the host system, the guest instruction instructing the at least one hardware processor to determine a result of applying an operator to an operand, wherein executing the guest instruction in the absence of the violation causes writing the result to a first location;

in response to determining whether executing the guest instruction causes the violation, when executing the guest instruction causes the violation, write the result to a second location distinct from the first location, the second location accessible to the computer security program; and

in response to writing the result to the second location, switch from executing the guest instruction to executing a computer security program, wherein the computer security program is configured to determine whether the violation is indicative of a computer security threat.

20. A non-transitory computer-readable medium storing instructions which, when executed by at least one hardware processor of a host system, cause the host system to form a computer security program configured to determine whether a violation of a memory access permission is indicative of a computer security threat, and wherein the at least one hardware processor is configurable to:

in response to receiving a guest instruction for execution, determine whether executing the guest instruction causes the violation, wherein the guest instruction executes within a guest virtual machine exposed by the host system, the guest instruction instructing the at least one hardware processor to determine a result of applying an operator to an operand, wherein executing the guest instruction in the absence of the violation causes writing the result to a first location;

in response to determining whether executing the guest instruction causes the violation, when executing the guest instruction causes the violation, write the result to a second location distinct from the first location, the second location accessible to the computer security program, and

in response to writing the result to the second location, switch from executing the guest instruction to executing the computer security program.