

CLAIMS

1. A computer system comprising at least one hardware processor configured to execute a set of guest virtual machines (VM) and to further execute a VM audit engine, the VM audit engine executing outside the set of guest VMs and configured, in response to receiving an audit request from a remote audit server, to:

insert an audit agent into a target VM of the set of the guest VMs, the audit agent configured to perform an audit of the target VM, the audit comprising an item selected from a group consisting of generating a list of legitimate computer programs installed for execution on the target VM and determining an amount of a hardware resource, the amount currently used by the target VM;

in response to inserting the audit agent, cause the target VM to execute the audit agent; and

in response to the target VM executing the audit agent, remove the audit agent from the target VM,

wherein inserting the audit agent comprises:

selecting a target memory page according to whether the target memory page contains a part of a driver of an operating system of the target VM,

writing a driver loader to the target memory page, the driver loader configured to load an audit driver into the target VM, the audit driver configured to perform the audit, and

configuring the target VM to switch, when a computer program executing within the target VM issues a system call, from executing the computer program to executing the driver loader.

2. The computer system of claim 1, wherein the audit further comprises determining a point in time when at least one computer program of the list of legitimate computer programs was installed.

3. The computer system of claim 1, wherein the audit further comprises generating a second list of legitimate computer programs, wherein all members of the second list are currently loaded in a volatile memory of the target VM.

4. The computer system of claim 1, wherein the hardware resource comprises a processing capacity of the at least one hardware processor.

5. The computer system of claim 1, wherein the hardware resource comprises a non-volatile storage device of the computer system.

6. The computer system of claim 1, wherein the VM audit engine is further configured to:

in preparation for inserting the audit agent, automatically detect a type of an operating system currently executing on the target VM; and

in response, configure the audit agent according to the type of the operating system.

7. The computer system of claim 1, wherein:

the audit request comprises an indicator of the target VM; and

the VM audit engine is configured to select the target VM from the set of guest VMs according to the audit request.

8. The computer system of claim 1, wherein the VM audit engine executes within an audit VM distinct from the target VM.

9. A method comprising employing at least one hardware processor of a computer system to execute a virtual machine (VM) audit engine outside a set of guest VMs executing on the computer system, wherein executing the VM audit engine comprises:

in response to receiving an audit request from a remote server, inserting an audit agent into a target VM of the set of guest VMs, the audit agent configured to perform an audit of the target VM, the audit comprising an item selected from a group consisting of generating a list of legitimate computer programs installed for execution on the target VM and determining an amount of a hardware resource, the amount currently used by the target VM;

in response to inserting the audit agent, causing the target VM to execute the audit agent; and

in response to the target VM executing the audit agent, removing the audit agent from the target VM,

5 wherein inserting the audit agent comprises:

selecting a target memory page according to whether the target memory page contains a part of a driver of an operating system of the target VM,

writing a driver loader to the target memory page, the driver loader configured to load an audit driver into the target VM, the audit driver configured to perform the audit, and

10 configuring the target VM to switch, when a computer program executing within the target VM issues a system call, from executing the computer program to executing the driver loader.

10. The method of claim 9, wherein the audit further comprises generating a second list of legitimate computer programs, wherein all members of the second list are currently loaded in
15 a volatile memory of the target VM.

11. The method of claim 9, wherein the hardware resource comprises a processing capacity of the at least one hardware processor.

12. The method of claim 9, wherein the hardware resource comprises a non-volatile storage device of the computer system.

20 13. The method of claim 9, comprising executing the VM audit engine within an audit VM distinct from the target VM.

14. The method of claim 9, further comprising:

in preparation for inserting the audit agent, automatically detecting a type of an operating system currently executing on the target VM; and

25 in response, configure the audit agent according to the type of the operating system.

15. The method of claim 9, wherein:

the audit request comprises an indicator of the target VM; and

the method further comprises selecting the target VM from the set of guest VMs according to the audit request.

16. A non-transitory computer-readable medium storing instructions which, when
5 executed by at least one hardware processor of a computer system, cause the computer system to form a virtual machine (VM) audit engine, the VM audit engine executing outside a set of guest VMs exposed on the computer system, wherein the VM audit engine is configured, in response to receiving an audit request from a remote audit server, to:

insert an audit agent into a target VM of the set of guest VMs, the audit agent
10 configured to perform an audit of the target VM, the audit comprising an item selected from a group consisting of generating a list of legitimate computer programs installed for execution on the target VM and determining an amount of a hardware resource, the amount currently used by the target VM;

in response to inserting the audit agent, cause the target VM to execute the audit agent;

15 and

in response to the target VM executing the audit agent, remove the audit agent from the target VM,

wherein inserting the audit agent comprises:

selecting a target memory page according to whether the target memory page contains
20 a part of a driver of an operating system of the target VM,

writing a driver loader to the target memory page, the driver loader configured to load an audit driver into the target VM, the audit driver configured to perform the audit, and

configuring the target VM to switch, when a computer program executing within the target VM issues a system call, from executing the computer program to executing the driver
25 loader.

17. The computer-readable medium of claim 16, wherein the instructions further cause at least one hardware processor of the computer system to form a hypervisor configured to expose the target VM on the computer system.