

CLAIMS

What is claimed is:

1. A computing device, comprising:
at least one processor; and
memory including instructions that, when executed by the at least one processor, cause the computing device to implement:
a hypervisor that manages one or more virtual machines and having access to a first portion of memory; and
a privileged service that is capable of suspending the hypervisor and running in system management mode (SMM) on the computing device, and the privileged service having access to at least a second portion of memory that is inaccessible to the hypervisor, the privileged service operable to:
store a key on the computing device;
receive a request to use the key from at least one of: the hypervisor or the one or more virtual machines; and
generate a response to the request, the response based at least in part on the key stored on the computing device.
2. The computing device of claim 1, wherein the privileged service is executed using at least one of:
a cryptographic processor, a remote management card, a baseboard management controller (BMC), a component executing in the system management mode (SMM), or a manageability engine.
3. The computing device of claim 1, wherein the second portion of memory is at least one of: a portion of main memory partitioned using one or more range registers, memory internal to one or more co-processors, memory attached to one or more co-processors, registers dedicated to one or more modes, or specific cryptographic key registers.

4. The computing device of claim 1, wherein the privileged service is further operable to:

notify an external entity in response to detecting that the hypervisor has been altered; or

delete the key in response to detecting that the hypervisor has been altered.

5. The computing device of claim 1, further comprising:

a component configured to submit the request to the privileged service by using a system management interrupt (SMI), the component residing in at least one of: the hypervisor or the virtual machine.

6. The computing device of claim 1, wherein the key is stored in a trusted platform module (TPM) and wherein the privileged service is further operable control access to the key stored in the TPM by the hypervisor and the one or more virtual machines.

7. The computing device of claim 1, wherein the privileged service is further operable to:

measure a first set of values associated with the hypervisor at boot time to verify the hypervisor.

8. The computing device of claim 7, wherein the privileged service is further operable to:

receive a first system management interrupt (SMI) from a virtual machine on the ~~host~~-computing device to verify the hypervisor;

measure, by an SMI handler, a second set of values associated with the hypervisor;

compare the second set of values with the first set of values by the SMI handler;

verify the hypervisor by the SMI handler if the second set of values match the first set of values measured at boot time; and

receive, from the virtual machine, a second SMI to retrieve the key or to store a new key.

9. The computing device of claim 1, wherein the privileged service is further operable to:

expose a virtual TPM to the one or more virtual machines, wherein the one or more virtual machines are operable to use a system managed interrupt (SMI) to access the key, the key being inaccessible to the hypervisor.

10. The computing device of claim 1, wherein generating the response is further based on authorization information associated with the cryptographic key.

11. The computing device of claim 1, wherein the request to use the key further includes at least one of:

a request that one or more computations be performed using the key; or
a request to transmit one or more messages encrypted or signed using the key.

12. A computer implemented method, comprising:

under the control of one or more computer systems configured with executable instructions,

storing, by a privileged service, a key on a host computing device, the host computing device including a hypervisor that manages one or more virtual machines, the privileged service that is capable of suspending the hypervisor and running in system management mode (SMM) on the host computing device, and the privileged service having access to at least a portion of memory inaccessible to the hypervisor;

receiving, by the privileged service, a signal that requests to use the key, the signal received from at least one of: the hypervisor or the one or more virtual machines; and

generating, by the privileged service, a response to the request, the response based at least in part on the key stored on the host computing device.

13. The computer implemented method of claim 12, further comprising:
measuring one or more values associated with the hypervisor;
detecting whether the hypervisor was altered based at least in part on the one or more values.

14. The computer implemented method of claim 13, further comprising: in response to detecting that the hypervisor was altered, performing at least one of:
sending a notification to an external entity, the notification indicating that the hypervisor has been altered; or
deleting the key.

15. The computer implemented method of claim 12, wherein storing the key further includes:
storing the key in a trusted platform module (TPM), wherein the privileged service is configured to have exclusive access to the TPM.

CLAIMS

What is claimed is:

1. A computing device, comprising:
at least one processor; and
memory including instructions that, when executed by the at least one processor, cause the computing device to implement:
a hypervisor that manages one or more virtual machines and having access to a first portion of memory; and
a privileged service that is capable of suspending the hypervisor and running in system management mode (SMM) on the computing device, and the privileged service having access to at least a second portion of memory that is inaccessible to the hypervisor, the privileged service operable to:
store a key on the computing device;
receive a request to use the key from at least one of: the hypervisor or the one or more virtual machines; and
generate a response to the request, the response based at least in part on the key stored on the computing device.
2. The computing device of claim 1, wherein the privileged service is executed using at least one of:
a cryptographic processor, a remote management card, a baseboard management controller (BMC), a component executing in the system management mode (SMM), or a manageability engine.
3. The computing device of claim 1, wherein the second portion of memory is at least one of: a portion of main memory partitioned using one or more range registers, memory internal to one or more co-processors, memory attached to one or more co-processors, registers dedicated to one or more modes, or specific cryptographic key registers.

4. The computing device of claim 1, wherein the privileged service is further operable to:

notify an external entity in response to detecting that the hypervisor has been altered; or

delete the key in response to detecting that the hypervisor has been altered.

5. The computing device of claim 1, further comprising:

a component configured to submit the request to the privileged service by using a system management interrupt (SMI), the component residing in at least one of: the hypervisor or the virtual machine.

6. The computing device of claim 1, wherein the key is stored in a trusted platform module (TPM) and wherein the privileged service is further operable control access to the key stored in the TPM by the hypervisor and the one or more virtual machines.

7. The computing device of claim 1, wherein the privileged service is further operable to:

measure a first set of values associated with the hypervisor at boot time to verify the hypervisor.

8. The computing device of claim 7, wherein the privileged service is further operable to:

receive a first system management interrupt (SMI) from a virtual machine on the computing device to verify the hypervisor;

measure, by an SMI handler, a second set of values associated with the hypervisor;

compare the second set of values with the first set of values by the SMI handler;

verify the hypervisor by the SMI handler if the second set of values match the first set of values measured at boot time; and

receive, from the virtual machine, a second SMI to retrieve the key or to store a new key.

9. The computing device of claim 1, wherein the privileged service is further operable to:

expose a virtual TPM to the one or more virtual machines, wherein the one or more virtual machines are operable to use a system managed interrupt (SMI) to access the key, the key being inaccessible to the hypervisor.

10. The computing device of claim 1, wherein generating the response is further based on authorization information associated with the cryptographic key.

11. The computing device of claim 1, wherein the request to use the key further includes at least one of:

a request that one or more computations be performed using the key; or
a request to transmit one or more messages encrypted or signed using the key.

12. A computer implemented method, comprising:

under the control of one or more computer systems configured with executable instructions,

storing, by a privileged service, a key on a host computing device, the host computing device including a hypervisor that manages one or more virtual machines, the privileged service that is capable of suspending the hypervisor and running in system management mode (SMM) on the host computing device, and the privileged service having access to at least a portion of memory inaccessible to the hypervisor;

receiving, by the privileged service, a signal that requests to use the key, the signal received from at least one of: the hypervisor or the one or more virtual machines; and

generating, by the privileged service, a response to the request, the response based at least in part on the key stored on the host computing device.

13. The computer implemented method of claim 12, further comprising:
measuring one or more values associated with the hypervisor;
detecting whether the hypervisor was altered based at least in part on the one or more values.

14. The computer implemented method of claim 13, further comprising: in response to detecting that the hypervisor was altered, performing at least one of:
sending a notification to an external entity, the notification indicating that the hypervisor has been altered; or
deleting the key.

15. The computer implemented method of claim 12, wherein storing the key further includes:
storing the key in a trusted platform module (TPM), wherein the privileged service is configured to have exclusive access to the TPM.