CLAIMS

1. A computer-implemented method, comprising:

obtaining, by a secure interface control in a computing system, wherein the secure interface control is communicatively coupled to a hypervisor, wherein the hypervisor manages one or more guests, metadata linked to an image of a secure guest of an owner and managed by the hypervisor, wherein the metadata comprises one or more controls, wherein each control of the one or more controls indicates to the secure interface control whether the hypervisor is permitted to execute an instance of a secure guest generated with the image in the computing system based on a presence or absence of one or more system settings in the computing system;

intercepting, by the secure interface control, a command by the hypervisor to initiate the instance of the secure guest from the image of the secure guest;

determining, by the secure interface control, the presence or the absence of the one or more system settings in the computing system;

determining, by the secure interface control, based on the one or more controls and the presence or the absence of the one or more system settings, if the hypervisor is permitted to execute the instance;

based on determining that the hypervisor is permitted to execute the instance:

enabling, by the secure interface control, initiation of the instance by the hypervisor, in the computing system, based on relaying the intercepted command to the hypervisor;

monitoring, by the secure interface control, the one or more system settings during runtime of the instance;

determining, by the secure interface control, that at least one setting of the one or more settings changed during the runtime;

identifying, by the secure interface control, a given control of the one or more controls relevant to the at least one setting;

determining, by the secure interface control, based on the at least one setting and the given control if the hypervisor is permitted to execute the instance; and

based on determining that the hypervisor is not permitted to execute the instance:

ignoring, by the secure interface control, the command.

2. The computer-implemented method of claim 1, wherein obtaining the metadata further comprises:

decrypting, by the secure interface control, a portion of the metadata linked to the image of the secure guest, wherein the metadata is integrity protected and the portion comprising a cryptographic measure of a boot image of the secure guest was encrypted by a key derived using a private key.

3. The computer-implemented method of claim 1 or 2, wherein the encrypted portion of the metadata comprises the one or more controls.

4. The computer-implemented method of one of claims 1 to 3, wherein each control of the one or more controls comprises an environmental constraint.

5. The computer-implemented method of claim 4, wherein the environmental constraints are selected from the group consisting of: systems configured to perform hardware measurements, and systems configured to use a non-system specific host key.

6. The computer-implemented method of claim 2, wherein the private key is owned by the secure interface control and used exclusively by the secure interface control.

7. The computer-implemented method of claim 6, wherein the key derived using the private key is shared between the secure interface control and the owner.

8. The computer-implemented method of one of claims 1 to 7, wherein the metadata comprises values derived from a boot image of the secure guest computed utilizing a collision resistant one-way function.

9. The computer-implemented method of one of claims 1 to 8, wherein the one or more controls each comprise a positive designation or a negative designation for a given system settings, wherein the positive designation indicates that the instance of the secure guest is permitted to execute in the computing system comprising the given system setting and the negative designation indicates that the instance of the secure guest is not permitted to execute in the computing system comprising the given system setting.

10. The computer-implemented method of one of claims 1 to 9, wherein the metadata is inaccessible to the instance of the secure guest.

11. The computer-implemented method of one of claims 1 to 10, wherein determining if the hypervisor is permitted to execute the instance further comprises:

identifying, by the secure interface control, in the one or more controls, a control relevant to a setting of the one or more system settings; and

determining, by the secure interface control, if the control enables or restricts executing the instance, based on the control.

12. The computer-implemented method of claim 1, further comprising:

based on determining that the hypervisor is not permitted to execute the instance, terminating, by the secure interface control, via the hypervisor, the instance.

13. The computer-implemented method of one of claims 1 to 12, wherein intercepting the command by the hypervisor to initiate the instance of the secure guest from the image of the secure guest further comprises:

performing, by the secure interface control, an integrity check on the metadata; and

based on successfully completing the integrity check, reading, by the secure interface control, the one or more controls in the metadata.

14. A computer program product comprising:

a computer readable storage medium readable by one or more processors and storing instructions for execution by the one or more processors for performing a method comprising:

obtaining, by the one or more processors in a computing system, wherein the one or more processors are communicatively coupled to a hypervisor, wherein the hypervisor manages one or more guests, metadata linked to an image of a secure guest of an owner and managed by the hypervisor, wherein the metadata comprises one or more controls, wherein each control of the one or more controls indicates to the one or more processors whether the hypervisor is permitted to execute an instance of a secure guest generated with the image in the computing system based on a presence or absence of one or more system settings in the computing system;

intercepting, by the one or more processors, a command by the hypervisor to initiate the instance of the secure guest from the image of the secure guest;

determining, by the one or more processors, the presence or the absence of the one or more system settings in the computing system;

determining, by the one or more processors, based on the one or more controls and the presence or the absence of the one or more system settings, if the hypervisor is permitted to execute the instance;

based on determining that the hypervisor is permitted to execute the instance:

enabling, by the one or more processors, initiation of the instance by the hypervisor, in the computing system, based on relaying the intercepted command to the hypervisor;

monitoring, by the secure interface control, the one or more system settings during runtime of the instance;

determining, by the secure interface control, that at least one setting of the one or more settings changed during the runtime;

identifying, by the secure interface control, a given control of the one or more controls relevant to the at least one setting;

determining, by the secure interface control, based on the at least one setting and the given control if the hypervisor is permitted to execute the instance; and

based on determining that the hypervisor is not permitted to execute the instance:

ignoring, by the one or more processors, the command.

15. The computer program product of claim 14, wherein obtaining the metadata further comprises:

decrypting, by the one or more processors, a portion of the metadata linked to the image of the secure guest, wherein the metadata is integrity protected and the portion comprising a cryptographic measure of a boot image of the secure guest was encrypted by a key derived using a private key.

16. The computer program product of claim 15, wherein the encrypted portion of the metadata comprises the one or more controls.

17. The computer program product of one of claims 14 to 16, wherein each control of the one or more controls comprises an environmental constraint.

18. The computer program product of claim 17, wherein the environmental constraints are selected from the group consisting of: systems configured to perform hardware measurements, and systems configured to use a non-system specific host key.

19. A computer system comprising:

a memory;

one or more processors in communication with the memory;

program instructions executable by the one or more processors via the memory to perform a method, the method comprising:

obtaining, by the one or more processors in the computing system, wherein the one or more processors are communicatively coupled to a hypervisor, wherein the hypervisor manages one or more guests, metadata linked to an image of a secure guest of an owner and managed by the hypervisor, wherein the metadata comprises one or more controls, wherein each control of the one or more controls indicates to the one or more processors whether the hypervisor is permitted to execute an instance of a secure guest generated with the image in the computing system based on a presence or absence of one or more system settings in the computing system;

intercepting, by the one or more processors, a command by the hypervisor to initiate the instance of the secure guest from the image of the secure guest;

determining, by the one or more processors, the presence or the absence of the one or more system settings in the computing system;

determining, by the one or more processors, based on the one or more controls and the presence or the absence of the one or more system settings, if the hypervisor is permitted to execute the instance;

based on determining that the hypervisor is permitted to execute the instance:

enabling, by the one or more processors, initiation of the instance by the hypervisor, in the computing system, based on relaying the intercepted command to the hypervisor;

monitoring, by the secure interface control, the one or more system settings during runtime of the instance;

determining, by the secure interface control, that at least one setting of the one or more settings changed during the runtime;

identifying, by the secure interface control, a given control of the one or more controls relevant to the at least one setting;

determining, by the secure interface control, based on the at least one setting and the given control if the hypervisor is permitted to execute the instance; and

based on determining that the hypervisor is not permitted to execute the instance:

ignoring, by the one or more processors, the command.