the host computing device is operable to decrypt the request using the private key stored on the host computing device.

6. The computer implemented method of claim 1, wherein the privileged operation is a request to modify a running memory image of the virtualization layer of the host computing device.

7. The computer implemented method of claim 1, wherein the privileged operation is a request to:

apply a patch to at least one of: a hypervisor or the kernel on the host computing device;

read a location in memory of a guest hosted on the host computing device;

modify one or more variables executing on the host computing device; or

shut down or reboot a guest executing on the host computing device.

8. The computer implemented method of claim 1, wherein the private key is stored in a trusted platform module (TPM) of the host computing device.

9. The computer implemented method of claim 1, wherein the request further includes at least one of:

a time stamp that limits a duration of time during which the request remains valid; or

a unique value that is associated with the host computing device.

10. The computer implemented method of claim 1, wherein the public key is associated with a set of privileged operations granted to a party that is in possession of the public key and wherein verifying the request includes determining that the privileged operation is included within the set.

11. A computing system, comprising:

at least one processor; and

memory including instructions that, when executed by the processor, cause the computing system to:

generate an asymmetric key pair including a public key and a private key upon booting;

receive, via an application programming interface (API), a request to execute a privileged operation on a virtualization layer of a host computing device, the request secured using at least ~~one key~~the public key; ~~and~~

attempt to verify the request by the virtualization layer of the host computing device; and

execute the privileged operation in the virtualization layer of the host computing device if the request is successfully verified.

12. The computing system of claim 11, wherein the request is secured by a signature generated using a second private key that is stored remotely with respect to the host computing device and wherein the request is verified using a second public key that is available to the host computing device.

13. The computing system of claim 12, wherein the host computing device is configured to use the second public key if the second public key is included in a certificate that is issued to an authorized party and signed by a certificate authority trusted by the host computing device.

14. The computing system of claim 11, wherein upon booting, the host computing device is configured to:

~~generate an asymmetric key pair including a second public key and a second private key; and~~

publish the ~~second~~ public key and store the ~~second~~ private key in volatile memory on the host computing device.

15. The computing system of claim 14, wherein publishing the ~~second~~ public key further includes:

sending a certificate signing request to a certificate authority to bind the ~~second~~ public key to a certificate.

the host computing device is operable to decrypt the request using the private key stored on the host computing device.

6. The computer implemented method of claim 1, wherein the privileged operation is a request to modify a running memory image of the virtualization layer of the host computing device.

7. The computer implemented method of claim 1, wherein the privileged operation is a request to:

apply a patch to at least one of: a hypervisor or the kernel on the host computing device;

read a location in memory of a guest hosted on the host computing device;

modify one or more variables executing on the host computing device; or

shut down or reboot a guest executing on the host computing device.

8. The computer implemented method of claim 1, wherein the private key is stored in a trusted platform module (TPM) of the host computing device.

9. The computer implemented method of claim 1, wherein the request further includes at least one of:

a time stamp that limits a duration of time during which the request remains valid; or

a unique value that is associated with the host computing device.

10. The computer implemented method of claim 1, wherein the public key is associated with a set of privileged operations granted to a party that is in possession of the public key and wherein verifying the request includes determining that the privileged operation is included within the set.

11. A computing system, comprising:

at least one processor; and

memory including instructions that, when executed by the processor, cause the computing system to:

generate an asymmetric key pair including a public key and a private key upon booting;