CLAIMS

What is claimed is:

1. A computer implemented method, comprising:

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

generating, by a monitoring service that monitors a plurality of host computing devices, a request to perform a privileged operation on a virtualization layer of a host computing device of the plurality of host computing devices;

obtaining a public key and including the public key in the request, the public key capable of being used to encrypt information, the public key having a corresponding private key that is capable of being used to decrypt the information encrypted using the public key;

submitting the request including the public key to the virtualization layer of the host computing device, the virtualization layer configured to execute the privileged operation to produce a result; and

wherein the virtualization layer is configured to encrypt the result of the privileged operation by using the public key provided with the request.

2. The computer implemented method of claim 1, wherein the virtualization layer is configured to encrypt the result before the result is communicated out of the virtualization layer of the host computing device.

3. The computer implemented method of claim 1, wherein the virtualization layer is configured to communicate the encrypted result to a location that is external with respect to the host computing device; and wherein the encrypted result is decrypted at the location by using a private key.

4. The computer implemented method of claim 1, wherein the request to perform the privileged operation is encrypted using a second key, and wherein the request is decryptable by the virtualization layer.

5. The computer implemented method of claim 1, wherein the request to perform the privileged operation is signed using a service private key, and wherein a signature of the request is verifiable by the virtualization layer using a service public key.

6. The computer implemented method of claim 5, further comprising:

obtaining a certificate including the service public key from a certificate authority (CA).

7. The computer implemented method of claim 1, wherein obtaining the public key further includes:

obtaining, using a certificate authority (CA), at least one certificate that certifies ownership of the public key.

8. ~~The computer implemented method of claim 1, wherein the request is generated by a monitoring service that monitors a plurality of host computing devices.~~

~~9.~~ The computer implemented method of claim ~~8~~1, further comprising:

detecting, by the monitoring service, that at least one of the plurality of host computing devices is operating abnormally based at least in part on a profile associated with the at least one of the plurality of host computing devices.

~~10~~9. The computer implemented method of claim 1, wherein the request is bound to a specified time duration.

~~11~~10. The computer implemented method of claim 1, wherein the privileged operation modifies a running memory image of the virtualization layer on the host computing device.

~~12~~11. The computer implemented method of claim 1, wherein the privileged operation further includes:

reading a location in memory on the host computing device, the location associated with the virtualization layer.

~~13~~12. A system, comprising:

a first computer system including at least one processor; and

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

receive, from a trusted party, a request to perform a privileged operation on a virtualization layer of a host computing device, the request including a public key, the public key capable of being used to encrypt information, the public key having a corresponding private key that is capable of being used to decrypt the information encrypted using the public key; and

issue the request to an application programming interface (API) of the host computing device, wherein the virtualization layer is configured to execute the privileged operation to produce a result and encrypt the result using the public key provided with the request, wherein the request to perform the privileged operation is encrypted using a second key, and wherein the request is decrypted by the virtualization layer.

~~14~~13. The system of claim ~~13~~12, further comprising:

the host computing device, wherein the host computing device includes at least one processor and memory including instructions that, when executed cause the host computing device to:

execute the privileged operation;

encrypt the result using the public key provided with the request; and

store the encrypted result in a predetermined location.

~~15. The computing system of claim 13, wherein the request to perform the privileged operation is encrypted using a second key, and wherein the request is decrypted by the virtualization layer.~~

CLAIMS

What is claimed is:

1. A computer implemented method, comprising:

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

generating, by a monitoring service that monitors a plurality of host computing devices, a request to perform a privileged operation on a virtualization layer of a host computing device of the plurality of host computing devices;

obtaining a public key and including the public key in the request, the public key capable of being used to encrypt information, the public key having a corresponding private key that is capable of being used to decrypt the information encrypted using the public key;

submitting the request including the public key to the virtualization layer of the host computing device, the virtualization layer configured to execute the privileged operation to produce a result; and

wherein the virtualization layer is configured to encrypt the result of the privileged operation by using the public key provided with the request.

2. The computer implemented method of claim 1, wherein the virtualization layer is configured to encrypt the result before the result is communicated out of the virtualization layer of the host computing device.

3. The computer implemented method of claim 1, wherein the virtualization layer is configured to communicate the encrypted result to a location that is external with respect to the host computing device; and wherein the encrypted result is decrypted at the location by using a private key.

4. The computer implemented method of claim 1, wherein the request to perform the privileged operation is encrypted using a second key, and wherein the request is decryptable by the virtualization layer.