METHOD OF AUTHORIZING AN OPERATION TO BE PERFORMED ON A TARGETED COMPUTING DEVICE

BACKGROUND

[1] The field of the present disclosure relates generally to mobile communication devices and, more specifically, to a mobile communication device that enables trusted operation of one or more isolated, virtualized operating systems running thereon.

[2] Mobile communication devices, such as smartphones, cellular phones, and personal digital assistants (PDAs) have grown in use and popularity among a variety of different types of users. At least some known devices include a central processing unit (CPU) that may be virtualized to simultaneously execute multiple operating systems (OSs) on one device. For example, a software program known as a hypervisor may be used to separate the different OSs by managing input/output (I/O) access operations transmitted between the OSs and hardware devices included in the computer system. More specifically, the hypervisor facilitates separating underlying hardware, such as the CPU and associated peripherals (e.g., display devices, touchscreens, and communications interfaces), from the OSs that run on the hardware.

[3] While device virtualization may facilitate separating one set of software from another set of software on known computing devices, the underlying platform may be susceptible to a variety of security vulnerabilities. Because of this, it has become increasingly important to those in the computer industry to increase the security of known computing devices. As such, it may be desirable to incorporate enhanced security into a device virtualization architecture.

BRIEF DESCRIPTION

[4] In one aspect, a method of authorizing an operation to be performed on a targeted computing device is provided. The method includes generating a request to perform an operation on the targeted computing device, signing the request with a private key of a first private, public key pair, transmitting the request to an authentication server, receiving an authorization response from the authentication server that includes the request and an authorization token, verifying the authorization response with a public key of a second private, public key pair, wherein the authorization response is signed with a private key of the second private, public key pair and transmitting the authorization response to the targeted computing device.

WHAT IS CLAIMED IS:

1. A method of authorizing an operation to be performed on a targeted computing device, said method comprising:

generating a request to perform an operation on the targeted computing device;

signing the request with a private key of a first private, public key pair;

transmitting the request to an authentication server;

receiving an authorization response from the authentication server that includes the request and an authorization token;

verifying the authorization response with a public key of a second private, public key pair, wherein the authorization response is signed with a private key of the second private, public key pair; and

transmitting the authorization response to the targeted computing device.

2. The method in accordance with Claim 1, wherein generating a request comprises generating the request to include at least one of an identification of the targeted computing device, the operation to be performed on the targeted computing device, a time period in which the operation will be performed, and a geographic location of the targeted computing device.

3. The method in accordance with Claim 1, wherein receiving an authorization response comprises receiving the authorization response that includes an authorization token having at least one of a predetermined authorization period, authorization to perform the operation on a predetermined targeted computing device, and authorization to perform predetermined operations on the targeted computing device.

4. The method in accordance with Claim 1, wherein transmitting the authorization response comprises transmitting the authorization response upon verification of the authorization response with the public key of the second private, public key pair.

5. The method in accordance with Claim 1 further comprising signing the authorization response with the private key of the first private, public key pair.

6. The method in accordance with Claim 1, wherein receiving the authorization response comprises determining whether the authorization token authorizes the requested operation.

7. The method in accordance with Claim 1, wherein transmitting the request comprises transporting the request to the authentication server via a removable media.

8. The method in accordance with Claim 1 further comprising:

receiving the request at the authentication server from a requesting device to perform an operation on the targeted computing device;

verifying the request with a public key of a first private, public key pair, wherein the request is signed by a private key of the first private, public key pair;

forming the authorization response that includes the request and the authorization token; and

transmitting the authorization response from the authentication server to the requesting device.

9. The method in accordance with Claim 8 further comprising determining whether to grant the request based on a security policy for the targeted computing device.

10. The method in accordance with Claim 9, wherein determining whether to grant the request comprises determining whether parameters for the operation to be performed align with the security policy for the targeted computing device.

11. The method in accordance with Claim 8 further comprising creating the authorization token at least one of prior to receiving the request to perform the operation on the targeted computing device and in response to verification of the request to perform the operation on the targeted computing device.

12. The method in accordance with Claim 8, wherein forming an authorization response comprises creating the authorization token to have at least one of a predetermined authorization period, authorization to perform the operation on a predetermined targeted computing device, and authorization to perform predetermined operations on the targeted computing device.

13. The method in accordance with Claim 8, further comprising:

receiving by the targeted computing device, the authorization response from the requesting device, the authorization response including the request to perform an operation on the targeted computing device and the authorization token;

verifying the authorization response with a public key of a private, public key pair, wherein the authorization response is signed by a private key of the private, public key pair; and

granting authorization to perform the operation upon verification of the authorization response.

14. A computer-implemented device for authorizing an operation to be performed on a targeted computing device, said computer-implemented device configured to perform the method of any of claims 1 to 6.