

MOBILE COMMUNICATION DEVICE AND METHOD OF OPERATING THEREOF

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 mobile communication device is provided. The mobile communication device includes a first trusted platform module; a second trusted platform module; a processor; and a non-transitory storage medium. The storage medium include instructions that cause said processor to establish a first root of trust for a first persona, the first persona comprising a first operating system and a first trusted execution environment; establish a second root of trust for a second persona, the second persona comprising a second operating system and a second trusted execution environment, wherein the first root of trust is separate from the second root of trust; store measurements defining the first root of trust for the first

persona in the first trusted platform module; store measurements defining the second root of trust for the second persona in the second trusted platform module; and load the first persona and the second persona using the roots of trust for the first and second personas, wherein the first persona can access components of the mobile communication device according to the first root of trust and the second persona can access components of the mobile communication device according to the second root of trust.

[5] In another aspect, a method of operating a mobile communication device is provided. The method includes establishing a first root of trust for a first persona, the first persona including a first operating system and a first trusted execution environment; establishing a second root of trust for a second persona, the second persona including a second operating system and a second trusted execution environment, wherein the first root of trust is separate from the second root of trust; storing measurements defining the first root of trust for the first persona in a first trusted platform module; storing measurements defining the second root of trust for the second persona in a second trusted platform module; and loading the first persona and the second persona using the roots of trust for the first and second personas, wherein the first persona can access components of the mobile communication device according to the first root of trust and the second persona can access components of the mobile communication device according to the second root of trust.

[6] In yet another aspect, a non-transitory computer readable medium storing computer-executable instructions thereon for operating a mobile communication device is provided. The mobile communication device includes a processor, a first trusted platform module, and a second trusted platform module. The computer-executable instructions cause the processor to establish a first root of trust for a first persona, the first persona including a first operating system and a first trusted execution environment; establish a second root of trust for a second persona, the second persona including a second operating system and a second trusted execution environment, wherein the first root of trust is separate from the second root of trust; store measurements defining the root of trust for the first persona in the first trusted platform module; store measurements defining the second root of trust for the second persona in the second trusted platform module; and load the first persona and the second persona using the roots of trust for the first and second personas, wherein the first persona can access components of the mobile communication device according to the first root of trust and the second persona can access components of the mobile communication device according to the second root of trust.

BRIEF DESCRIPTION OF THE DRAWINGS

[7] Figure 1 is a front perspective view of an exemplary mobile communication device.

[8] Figure 2 is a back perspective view of the mobile communication device shown in Figure 1.

[9] Figure 3 is a schematic illustration of an exemplary hardware architecture that may be used with the mobile communication device shown in Figure 1.

CLAIMS

1. A mobile communication device comprising:
 - a first trusted platform module;
 - a second trusted platform module;
 - a processor; and
 - a non-transitory storage medium comprising instructions that cause said processor to:
 - establish a first root of trust for a first persona, the first persona comprising a first operating system and a first trusted execution environment;
 - establish a second root of trust for a second persona, the second persona comprising a second operating system and a second trusted execution environment, wherein the first root of trust is separate from the second root of trust;
 - store measurements defining the first root of trust for the first persona in the first trusted platform module;
 - store measurements defining the second root of trust for the second persona in the second trusted platform module; and
 - load the first persona and the second persona using the roots of trust for the first and second personas, wherein the first persona can access components of the mobile communication device according to the first root of trust and the second persona can access components of the mobile communication device according to the second root of trust.
2. The device in accordance with claim 1, wherein said storage medium further comprises instructions that cause said processor to establish mutual trust between the first trusted execution environment and the second trusted execution environment such that the first persona is coupled in communication with the second persona.
3. The device in accordance with claim 2 further comprising a high assurance guard that facilitates restricting transfer of data between the first persona and the second persona when the first persona is coupled in communication with the second persona.

4. The device in accordance with claim 1, wherein said storage medium further comprises instructions that cause said processor to transfer control of the first trusted platform module to the first persona and transfer control of the second trusted platform module to the second persona after the first and second personas have been loaded.

5. The device in accordance with claim 4, wherein the first trusted execution environment has exclusive access to the first trusted platform module and the second trusted execution environment has exclusive access to the second trusted platform module.

6. The device in accordance with claim 1, wherein said storage medium further comprises instructions that cause said processor to validate an image of the first operating system and the second operating system against the associated roots of trust for the first persona and the second persona during loading.

7. The device in accordance with claim 1, wherein said storage medium further comprises instructions that cause said processor execute the first persona and the second persona in contexts that are isolated from each other.

8. A method of operating a mobile communication device, said method comprising:
establishing a first root of trust for a first persona, the first persona including a first operating system and a first trusted execution environment;
establishing a second root of trust for a second persona, the second persona including a second operating system and a second trusted execution environment, wherein the first root of trust is separate from the second root of trust;
storing measurements defining the first root of trust for the first persona in a first trusted platform module;
storing measurements defining the second root of trust for the second persona in a second trusted platform module; and
loading the first persona and the second persona using the roots of trust for the first and second personas, wherein the first persona can access components of the mobile communication device according to the first root of trust and the second persona can access components of the

mobile communication device according to the second root of trust.

9. The method in accordance with claim 8 further comprising establishing mutual trust between the first trusted execution environment and the second trusted execution environment such that the first persona is coupled in communication with the second persona.

10. The method in accordance with claim 8, wherein loading the first persona and the second persona comprises loading an underlying operating system with a boot loader signed by a device manufacturer root of trust.

11. The method in accordance with claim 8, wherein establishing the roots of trust for the first and second personas comprises validating an image of the first operating system and the second operating system against the roots of trust for the first and second personas during loading.

12. The method in accordance with claim 8 further comprising transferring control of the first trusted platform module to the first persona and transferring control of the second trusted platform module to the second persona after the first and second personas have been loaded.

13. The method in accordance with claim 8, wherein establishing a root of trust for the first and second personas comprises:

measuring software components used to establish the first and second persona roots of trust; and

extending the measurements into the first and second trusted platform modules, wherein the measurements for the first trust anchor extend into the first trusted platform module and the measurements for the second trust anchor extend into the second trusted platform module.

14. The method in accordance with claim 8 further comprising:

defining a security policy for the first persona and the second persona, wherein the security policies define how the first persona and the second persona access physical devices on the mobile communication device; and

enforcing the security policies with a security supervisor.

15. The method in accordance with claim 14, wherein enforcing the security policies comprises at least one of:

enabling exclusive access for one of the first persona and the second persona to at least one of the physical devices;

enabling shared access between the first persona and the second persona to at least one of the physical devices; and

denying access of at least one of the physical devices to one of the first persona and the second persona.

16. A non-transitory computer readable medium storing computer-executable instructions thereon for operating a mobile communication device that includes a processor, a first trusted platform module, and a second trusted platform module, the computer-executable instructions cause the processor to:

establish a first root of trust for a first persona, the first persona including a first operating system and a first trusted execution environment;

establish a second root of trust for a second persona, the second persona including a second operating system and a second trusted execution environment, wherein the first root of trust is separate from the second root of trust;

store measurements defining the root of trust for the first persona in the first trusted platform module;

store measurements defining the second root of trust for the second persona in the second trusted platform module; and

load the first persona and the second persona using the roots of trust for the first and second personas, wherein the first persona can access components of the mobile communication device according to the first root of trust and the second persona can access components of the mobile communication device according to the second root of trust.

17. The non-transitory computer readable medium in accordance with claim 16 further comprising computer-executable instructions that cause the processor to:

establish mutual trust between the first trusted execution environment and the second trusted execution environment such that the first persona is coupled in communication with the second persona.

18. The non-transitory computer readable medium in accordance with claim 16 further comprising computer-executable instructions that cause the processor to:

load an underlying operating system with a boot loader signed by a device manufacturer root of trust,

19. The non-transitory computer readable medium in accordance with claim 16 further comprising computer-executable instructions that cause the processor to:

transfer control of the first trusted platform module to the first persona and transfer control of the second trusted platform module to the second persona after the first and second personas have been loaded.

20. The non-transitory computer readable medium in accordance with claim 16 further comprising computer-executable instructions that cause the processor to:

define a security policy for the first persona and the second persona, wherein the security policies define how the first persona and the second persona access physical devices on the mobile communication device; and

enforce the security policies with a security supervisor.