May 15, 2017

Secure Separation and Control of Multiple Virtual Machines

David Weekly

Secure Separation and Control of Multiple Virtual Machines

David Weekly

Abstract:

A hypervisor provides secure separation of multiple virtual machines on a device, thus removing conflicts when using the device for multiple purposes, including business and personal use. The hypervisor ensures security and privacy amongst the multiple virtual machines and prevents malicious attacks on one virtual machine from threatening another virtual machine. A switch provides a dedicated interface to the hypervisor, enabling secure switching between the multiple virtual machines. In addition, an indicator enables the hypervisor to identify an active virtual machine. Furthermore, the hypervisor hibernates inactive virtual machines in order to conserve power and provide another layer of protection against malicious attacks.

Keywords: virtual machine, modes, hypervisor, switch, security, hibernation

Background:

It is convenient to have a single device to support both business and personal use. However, conflicts often arise. For example, corporations require control over the device to protect corporate resources and secrets. These controls can restrict available resources by limiting which personal applications a user may download and/or access on the device. In addition, background security programs can slow down operations of the device, causing the user frustration when operating the device for personal use. Furthermore, these corporate controls can invade personal privacy and cause the user to hesitate using the device for activities involving personal communications, managing appointments, and taking pictures.

Description:

To address this problem, a device is configured to provide secure low-level and unambiguous separation of multiple virtual machines. Furthermore, the device provides a user authoritative control over which virtual machine is active. Figure 1 depicts an example device, which is described in further detail below.

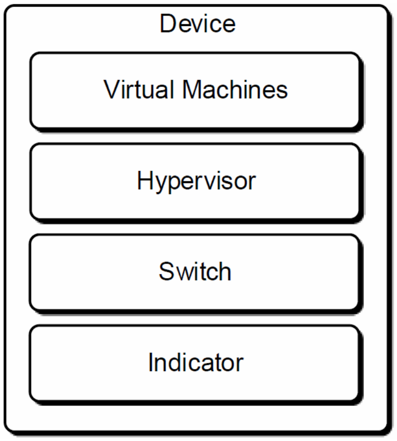

Figure 1

The device in Figure 1 can be one of a variety of devices, such as a mobile computing device, a smartphone, a computing watch, computing spectacles, or a tablet computer. Other computing devices and systems, such as a wearable computing device, a server, or desktop computer, may also be used.

The device is configured to run multiple virtual machines. The virtual machines represent individual modes, configurations, and/or profiles on the device. The virtual machines can be associated with different hardware (e.g., separate memories, different subscriber identify modules (SIMs)), software (e.g., operating systems, applications), and security settings. While virtual machines are described, other implementations, such as containers, can also be used. The multiple virtual machines can be created for specific uses, such as for business, personal, shopping, entertainment, finance, kids, guests, sandbox for programming, debugging, backup, and so forth. As another example, for a dual subscriber identify module (SIM) device, one SIM can be dedicated for work use while the other SIM is dedicated for personal use. In this way, the user can use a single device to receive both business and personal communications.

The device includes a hypervisor to separate and manage the multiple virtual machines at a low level. The hypervisor ensures none of the processes and data associated with one virtual machine can be accessed by another. By preventing the multiple virtual machines from interacting with each other, the hypervisor ensures security and privacy amongst the multiple virtual machines. Furthermore, the hypervisor provides confidence that malicious attacks on one virtual machine cannot threaten another virtual machine. In this way, a user can use one of the virtual machines for higher security risk activities such as trying out new applications and internet searching and have confidence that another virtual machine used for securely accessing important information, such as bank accounts, will remain secure even if the higher security risk virtual machine is compromised. While a hypervisor is described, other methods of securely separating the individual modes and/or profiles can also be used.

The hypervisor is configured to have a small set of responsibilities in order to help reduce an opportunity for malicious attacks to escalate and run in a virtual machine or at the hypervisor level. Furthermore, a trusted boot process, which may be assisted using Trusted Platform Module (TPM), provides assurance that the hypervisor is trusted. The trusted boot process is illustrated in Figure 2 whereby the hypervisor can also act as a link in the chain of trust to validate software signatures before loading software associated with the multiple virtual machines. The hypervisor can also enable both un-signed and signed software to load.

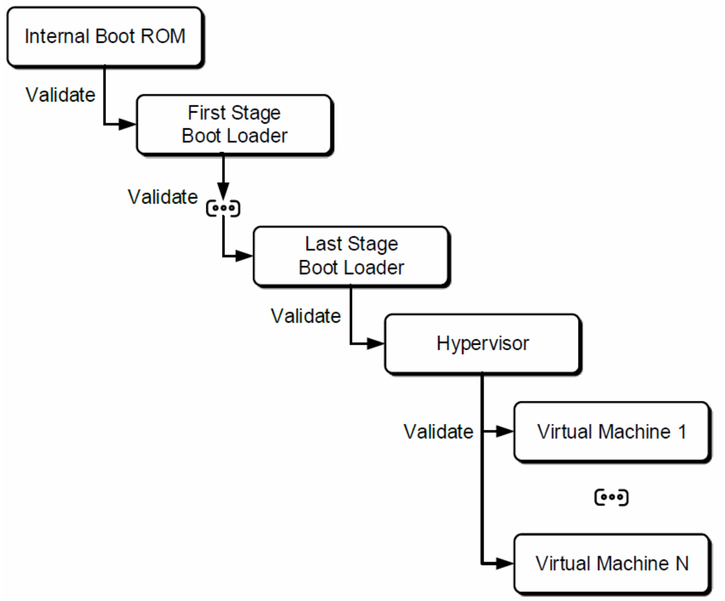

Figure 2

Returning to Figure 1, the device includes a switch, which acts as a dedicated interface to the hypervisor. The switch enables a user to switch between the multiple virtual machines. In order to provide the user with authoritative control, the switch is implemented using hardware and is only accessible by the hypervisor. This provides another layer of security, whereby malicious software cannot override the switch. The hypervisor monitors the switch and determines which virtual machine is selected by the user.

The device also includes an indicator to provide feedback to the user, identifying which virtual machine is active. The virtual machine indicator can be a physical label on the switch or an indicator provided by the hypervisor. As an example, the hypervisor can turn on an LED light associated with an active virtual machine.

The hypervisor operates with the switch and indicator to provide the user control in switching between multiple virtual machines. The hypervisor monitors the switch and when the hypervisor detects a new virtual machine selection, the hypervisor performs operations described in Figure 3.

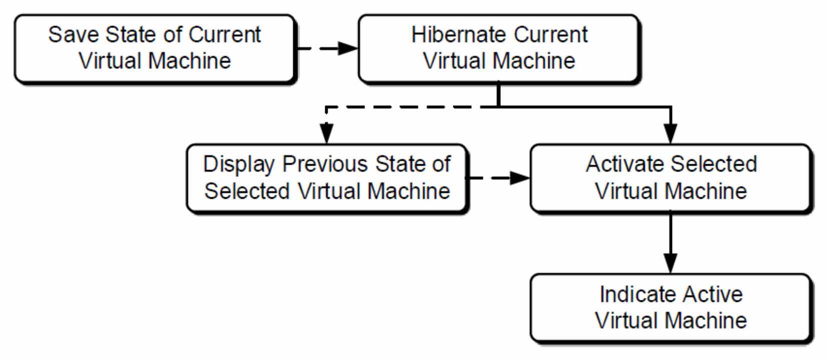
Save State of Current Virtual Machine
Hibernate Current Virtual Machine
Display Previous State of Selected Virtual Machine
Activate Selected Virtual Machine
Indicate Active Virtual Machine

Figure 3

To switch from a current virtual machine to the selected virtual machine, the hypervisor first places the current virtual machine in hibernation (e.g., sleep mode, low-power mode). Hibernation allows the device to conserve power and reduce battery drain. Another advantage involves protecting the hibernating virtual machine from timing attacks conducted from an active virtual machine. While in hibernation mode, the timing attacks are unable to observe and deduce activity corresponding to the hibernating virtual machine. In this way, hibernation provides another level of separation between the multiple virtual machines and ensures that a highly trusted process is not running at the same time as an untrusted process.

Optionally, before placing the current virtual machine in hibernation, the hypervisor can save a state of the current virtual machine, such as saving a screenshot. This allows the hypervisor to provide immediate visual feedback to the user when the current virtual machine is made active again.

After placing the current virtual machine in hibernation, the hypervisor activates the virtual machine selected through the switch. Optionally, before or during the process of activating the selected virtual machine, the hypervisor can display a previous state of the selected virtual machine to provide the user immediate feedback and enable fast switching between the multiple virtual machines.

Next, the hypervisor provides the user feedback by using the indicator to identify the selected virtual machine is active. As described above, this can involve a specific indicator from the hypervisor, such as turning on an LED light associated with the active virtual machine.

The hypervisor can also include additional functionality to periodically wake up high priority background tasks on the hibernating virtual machines and provide notification to the user regarding high priority items. As an example, the hypervisor can enable a hibernating virtual machine to check for recent communications, such as text messages, phone calls, and emails. Responsive to detecting a recent communication, the hypervisor can notify the user of an available communication. For example, the hypervisor can notify the user by flashing an LED associated with the hibernating virtual machine. A multi-core processor or multiprocessor system-on-chip (SoC) can be used such that the virtual machine's background tasks are executed on a different core than the virtual machine's foreground (e.g., main) tasks. As an example, the big.LITTLE^{TM} computing architecture can be used to enable a slower battery-saving processor core to execute the background tasks and fast cores to execute the foreground tasks. By separating the background tasks and the foreground tasks on different cores, the background tasks are better protected from security threats that may compromise the fast cores.

Examples:

A variety of switches can be used on the device. Examples include a rocker switch as shown in Figure 4, a toggle switch as shown in Figure 5, or a button. These examples are particularly useful when the number of virtual machines is small.

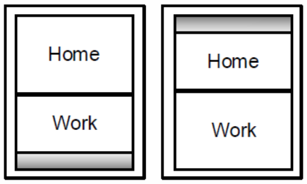

Figure 4

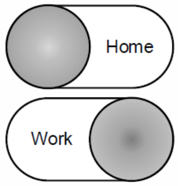

Figure 5

For supporting a large number of virtual machines, the device can include a rotary dial for switching between the multiple virtual machines, as shown in Figure 6. The rotary dial can include labels identifying the multiple virtual machines.

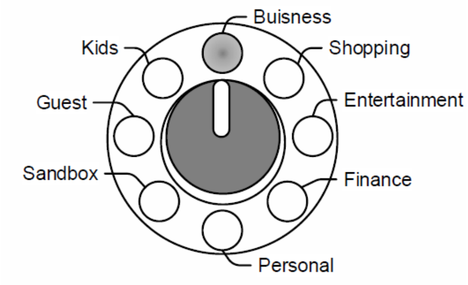

Figure 6

The switches in Figure 4, Figure 5, and Figure 6 can also include lights, such as LEDs, which the hypervisor can turn on/off to identify which virtual machine is active and/or provide notification of high priority items available on hibernating virtual machines. Different-colored lights can be used to further distinguish the multiple virtual machines.

Another type of switch can include a small display on the device. The small display is only controllable by the hypervisor. Through the display, the hypervisor can receive commands from the user and identify the active virtual machine. The hypervisor can also provide notifications on the display to indicate high-priority items available on hibernating virtual machines.

As another example, the device can also include dedicated screens for each of the virtual machines. For example, a mobile computing device can have a screen on a front side dedicated for business use and another screen on a reverse side dedicated for personal use, as illustrated in Figure 7. Bezels on each side can have a unique design or color associated with the corresponding virtual machine to indicate to a user which side corresponds with which virtual machine.

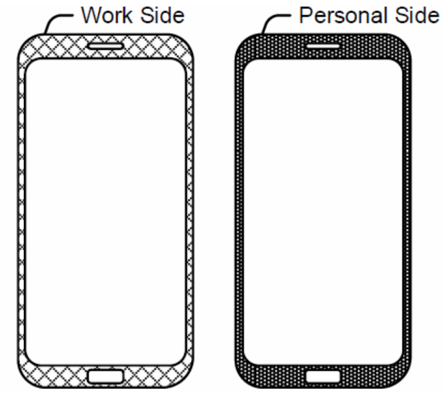

Figure 7

In Figure 7, the hypervisor can use built-in hardware to determine which virtual machine is active. For example, the device can include a gyroscope to indicate orientation of the device. As another example, the device can include a camera and a face detector to indicate which side is facing a user. The hypervisor can also turn off the inactive screen in order to save energy.