CLEARANCE OF BARE METAL RESOURCE TO TRUSTED STATE USABLE IN CLOUD COMPUTING

PRIORITY

The present application claims priority to U.S. provisional patent application Ser. No. 62/630,534, filed Feb. 14, 2018, which is incorporated by reference in its entirety.

BACKGROUND

[0001] Cloud computing typically involves the delivery of computing services, which may involve servers, storage, databases, networking, software, etc., over the Internet. Companies offering these computing services are called cloud providers and typically charge for cloud computing services based on usage.

[0002] Often, cloud providers use virtualization to implement a reusable pool of computing resources that can be assigned to different tenants. Virtualization is a technology that separates physical infrastructure to create various dedicated resources, such as virtual machines (VMs), that can run different instances of operating systems and applications on the same server. Using server virtualization, cloud providers can maximize the use of server resources and reduce the number of servers required. Also, VMs may run as separate, isolated units, thus providing fault and security isolation. Cloud providers may rely on virtualization technology to protect hardware from various intrusive attacks, such as attacks caused by firmware malware, bios-level hypervisor attacks, BIOS (basic input/output system)/firmware overwrite and denial of service attacks. Commonly, non-volatile memory modules on a system board are the target for such attacks, because targeting the non-volatile

What is claimed is:

1. A bare metal resource comprising:

a trusted portion including a first processing circuit, a clearance manager, and an image repository storing a known good basic input/output system (BIOS);; and

an untrusted portion including a second processing circuit and storage devices storing untrusted software that includes an accessible ~~basic input/output system (~~BIOS~~)~~,

wherein, in response to a signal indicating that the bare metal resource is to be reassigned or that the bare metal resource has failed, the first processing circuit in the trusted portion is triggered by the signal to reboot the bare metal resource from the trusted portion and cause ~~-~~the clearance manager in the trusted portion ~~is executable by the processing circuit during bootup of the bare metal resource prior to the BIOS~~ to perform a clearance process on the untrusted portion to place the bare metal resource in a known good state prior to providing access to the bare metal resource, the clearance process including deleting data stored in the ~~the BIOS in the untrusted portion and loading a trusted BIOS from the image repository on a~~ storage devices of the untrusted portion and restoring the accessible BIOS in the untrusted portion by replacing the accessible BIOS in ~~storing~~ the untrusted portion with the known good BIOS from the image repository of the trusted portion, and ~~software, to place the bare metal resource in a trusted state.~~

in response to verifying that the clearance process has been completed, the second processing circuit in the untrusted portion reboots the bare metal resource from the untrusted portion using the restored accessible BIOS in the untrusted portion.

2. The bare metal resource of claim 1 , wherein ~~to perform~~ the clearance process further includes, deleting ~~the clearance manager wipes~~ the untrusted software, including ~~and data from storage devices of the untrusted portion, and loads at least one trusted image, including~~ the accessible ~~trusted~~ BIOS, previously stored ~~from the image repository to at least one of the storage devices of~~ in the untrusted portion.

3. The bare metal resource of claim 1~~2~~, wherein the ~~at least~~ clearance process further includes loading ~~one trusted image comprises at least one of a device driver and~~ firmware from the image repository of the trusted portion into a storage device of the storage devices of the untrusted portion.

4. The bare metal resource of claim 12, wherein ~~to perform~~ the clearance process further includes setting ~~, the clearance manager sets~~ a state of a real-time clock to a valid default value.

5. The bare metal resource of claim 1, wherein ~~the bare metal resource is a computing resource available to a tenant of a cloud provider, and~~

the untrusted portion is accessible by a new ~~the~~ tenant via a network after the bare metal resource is rebooted from the untrusted portion. ~~placed in the trusted state.~~

6. The bare metal resource of claim 1, wherein the trusted portion and the untrusted portion are not simultaneously operational.

7.~~6.~~ The bare metal resource of claim 5, wherein the bare metal resource is communicatively coupled to a trusted infrastructure device in a control plane of a ~~the~~ cloud provider via an out-of-band channel, and

the bare metal resource is configured to receive the ~~a~~ signal indicating that the bare metal resource is to be reassigned or that the bare metal resource has failed from the trusted infrastructure device to invoke the clearance process.

8.~~7.~~ The bare metal resource of claim 7~~6~~, wherein the bare metal resource is configured to receive a verification that the clearance process has been completed ~~second signal~~ from the trusted infrastructure device via the out-of-band channel, after the trusted infrastructure device has verified that the clearance process is completed and

~~verifies~~ the bare metal resource is in the known good ~~trusted~~ state, to cause the bare metal resource to reboot from the ~~trusted BIOS loaded in the~~ untrusted portion.

9.~~8.~~ The bare metal resource of claim 7~~6~~, wherein the trusted infrastructure device runs a timer ~~to determine whether~~ when the clearance process begins to determine whether the clearance process has been completed or is stalled.

10.~~9.~~ The bare metal resource of claim 7~~6~~, wherein the trusted infrastructure device is a rack controller, and the out-of-band channel comprises a wired connection between the rack controller and a connector on a system board of the bare metal resource.

~~10. The bare metal resource of claim 1 , wherein the trusted portion and the untrusted portion are not simultaneously operational.~~

11. A bare metal resource in a pool of computing resources, the bare metal resource comprising:

a trusted portion including a memory storing a clearance manager, an image repository storing a known good basic input/output system (BIOS)~~images~~, and a first processing circuit to execute the clearance manager, wherein the trusted portion is inaccessible to a new tenant;

an untrusted portion, accessible to the new tenant when the bare metal resource is assigned ~~provisioned~~ to the new tenant, including a second processing circuit and

storage device storing ~~hardware and~~ untrusted software that comprises an accessible ~~basic input/output system (~~BIOS~~)~~; and

a communication interface communicatively coupled to an external ~~trusted infrastructure~~ device ~~of a cloud provider via an out-of-band channel~~,

wherein in response to receiving a first signal, from the external ~~trusted infrastructure~~ device, indicating that ~~via the out-of-band channel,~~ the bare metal resource is to be reassigned to the new tenant or that the bare metal resource has failed, the first processing circuit in the trusted portion is triggered by the first signal to reboot the bare metal resource from the trusted portion and cause ~~configured to boot from~~ the clearance manager in the trusted portion~~, and the clearance manager is configured~~ to perform a clearance process on the untrusted portion to place the bare metal resource in a known good state prior to providing access to the bare metal resource , the clearance process including deleting data stored in the storage devices of the untrusted portion by a previous tenant and restoring the accessible ~~-~~BIOS in the untrusted portion by replacing the accessible ~~and loading a trusted~~ BIOS ~~from the image repository on a storage device~~ in the untrusted portion with the known good BIOS from the image repository of the trusted portion, and ~~to place the bare metal resource in a trusted state.~~

in response to verifying that the clearance process has been completed, the second processing circuit in the untrusted portion reboots the bare metal resource from the untrusted portion using the restored accessible BIOS in the untrusted portion.

12. The bare metal resource of claim 11, wherein the external device is a trusted infrastructure device of a cloud service provider.

13. The bare metal resource of claim 11, wherein the clearance process further includes deleting the untrusted software, including the accessible BIOS, previously stored in the untrusted portion.

14. The bare metal resource of claim 11, wherein the external device runs a timer to determine whether the clearance process has been completed or is stalled.

15. The bare metal resource of claim 11, wherein the external device is a rack controller communicatively coupled to the bare metal resource via an out-of-band channel, and wherein the out-of-band channel comprises a wired connection between the rack controller and a connector on a system board of the bare metal resource.

16. The bare metal resource of claim 11, wherein the trusted portion and the untrusted portion are not simultaneously operational.

17. The bare metal resource of claim 11, wherein the trusted portion and the untrusted portion are on a mother-board of the bare metal resource.

~~12. The bare metal resource of claim 11, wherein the bare metal resource is configured to receiye a second signal from the trusted infrastructure device via the out-of-band channel to cause the bare metal resource to boot from the trusted BIOS loaded in the untrusted portion after the bare metal resource is in the trusted state.~~

18.~~13.~~ A method comprising:

receiving, from a trusted infrastructure device ~~of a cloud provider~~, a first signal indicating that ~~at~~ a bare metal resource is to be reassigned or that the bare metal resource has failed~~operable to be provisioned to a tenant of the cloud provider~~;

~~triggering a boot of the bare metal resource from a trusted portion of the bare metal resource responsive to the signal;~~

in response to the first signal indicating that the bare metal resource is to be reassigned or that the bare metal resource has failed, causing a first processor in a trusted portion of the bare metal resource to reboot the bare metal resource from the trusted portion

and causing a clearance manager in the trusted portion to perform a clearance process on an untrusted portion of the bare metal resource to place the bare metal resource in a known good state prior to providing access to the bare metal resource, wherein the clearance process includes deleting data stored in storage devices of the untrusted portion by a previous tenant and restoring an accessible basic input/output system (BIOS) in the untrusted portion by replacing the accessible BIOS in the untrusted portion with a known good BIOS from an image repository of the trusted portion of the bare metal resource; and

in response to verifying that the clearance process has been completed, causing a second processor in the untrusted portion of the bare metal resource to reboot the bare metal resource from the untrusted portion using the restored accessible BIOS in the untrusted portion.

~~performing, by a clearance manager in the trusted portion, a clearance process to wipe storage devices of an untrusted portion of the bare metal resource and to load a known good image of a basic input/output system (BIOS) from an image repository of the trusted portion of the bare metal resource to the untrusted portion; and~~

~~rebooting the bare metal resource from the BIOS loaded on the untrusted portion from the image repository.~~

19.~~14.~~ The method of claim 18~~13~~, wherein the trusted infrastructure device transmits a second ~~the~~ signal to the bare metal resource indicating ~~responsive to an indication~~ that the clearance process has been verified to be completed to cause the second processor to reboot~~bare metal resource is being released from the tenant or an indication that~~ the bare metal resource from the untrusted portion. ~~is in a non-operational state.~~

20. The method of claim 18, wherein the trusted infrastructure device runs a timer to determine whether the clearance process has been completed.

~~15. The method of claim 13, wherein rebooting the bare metal resource is in response to receiving a second signal from the trusted infrastructure device, wherein the trusted infrastructure device transmits the second signal to the bare metal resource after verifying the clearance process is successfully completed.~~